Hacking with Nintendo DS

착이 @ Security First
Department of Information Security Engineering
SoonChunHyang University

Hacking with Nintendo DS

- NDS(Nintendo DS)의 특징
  터치스크린과 무선랜 디바이스를 이용하여 원격의 PC와 통신 가능
  사용자가 직접, 원하는 프로그램 개발 가능 (Homebrew, 홈브류)
- 해킹 도구로써 사용 가능

Agenda

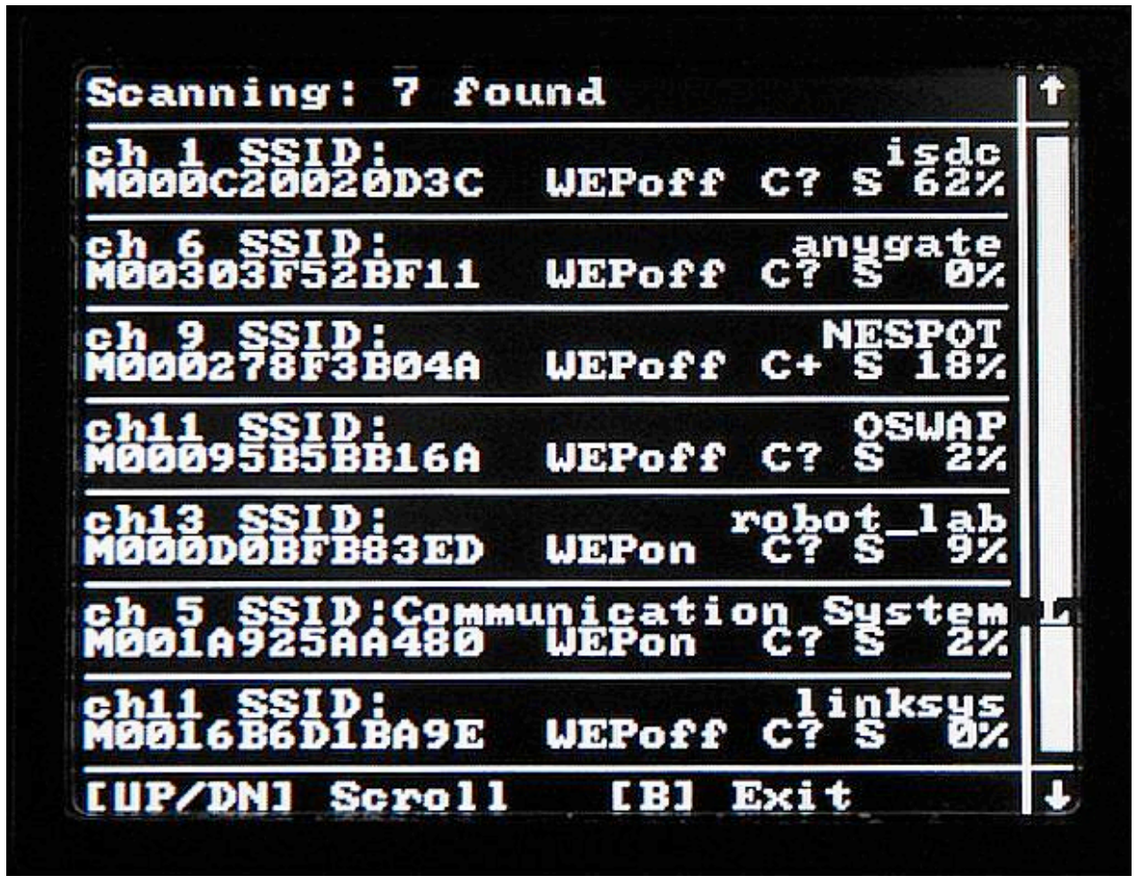
- 이미 존재하는 홈브류 사용하기
- 공격용 홈브류를 만들어 사용하기
- 예상 시나리오
- 대응방안

Part One

이미 존재하는 홈브류 사용하기

Wireless Netwrok Hacking

- DS Wifi
  NDS용 홈브류의 Wi-Fi 사용을 가능하게 하는 라이브러리
  http://akkit.org/dswifi
- War Driving
  주변의 Wi-Fi 네트워크 검색 및 접속 테스트 가능
- Packet Sniffing (imperfectly)
  무선 네트워크 스니핑



Linux Client

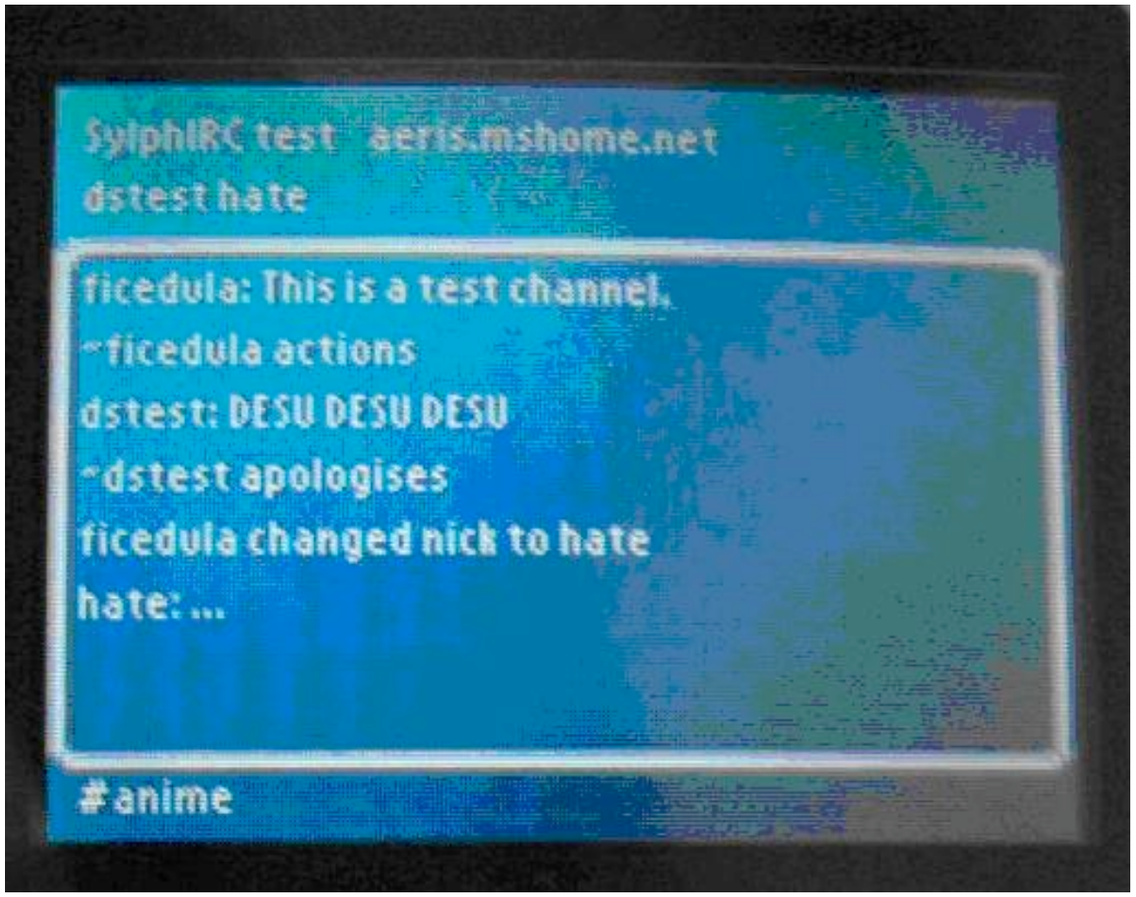
- **DSLinux**
  NDS에서 리눅스를 사용하기 위한 프로젝트, http://dslinux.org/
- **Telnet, SSH, FTP client**
  공격 당한 시스템이나 공격을 하기 위한 시스템에 접속 가능

System Remote Control

- **Win2DS, PointyRemote**
  터치스크린을 이용하여 VNC와 비슷하게 모니터링, 키보드, 마우스 제어
  http://win2ds.1emulation.com/
- **Victim System Control**
  공격당한 시스템에 Win2DS 서버를 설치하면 NDS로 제어 가능

Communication

- ircDS
  NDS에서 동작하는 IRC 클라이언트
  http://HtheB.area-ds.com
- Beup
  NDS에서 동작하는 MSN 클라이언트
- BOT Control
  IRC나 MSN을 이용하는 BOT을 NDS로 제어 가능



- FTP server
  DSFTP, 간단한 FTP 서버
  원격시스템에 필요한 파일을 전송할 때 이용 가능
  http://giesler.biz/bjoern/en/sw_dsftp.html

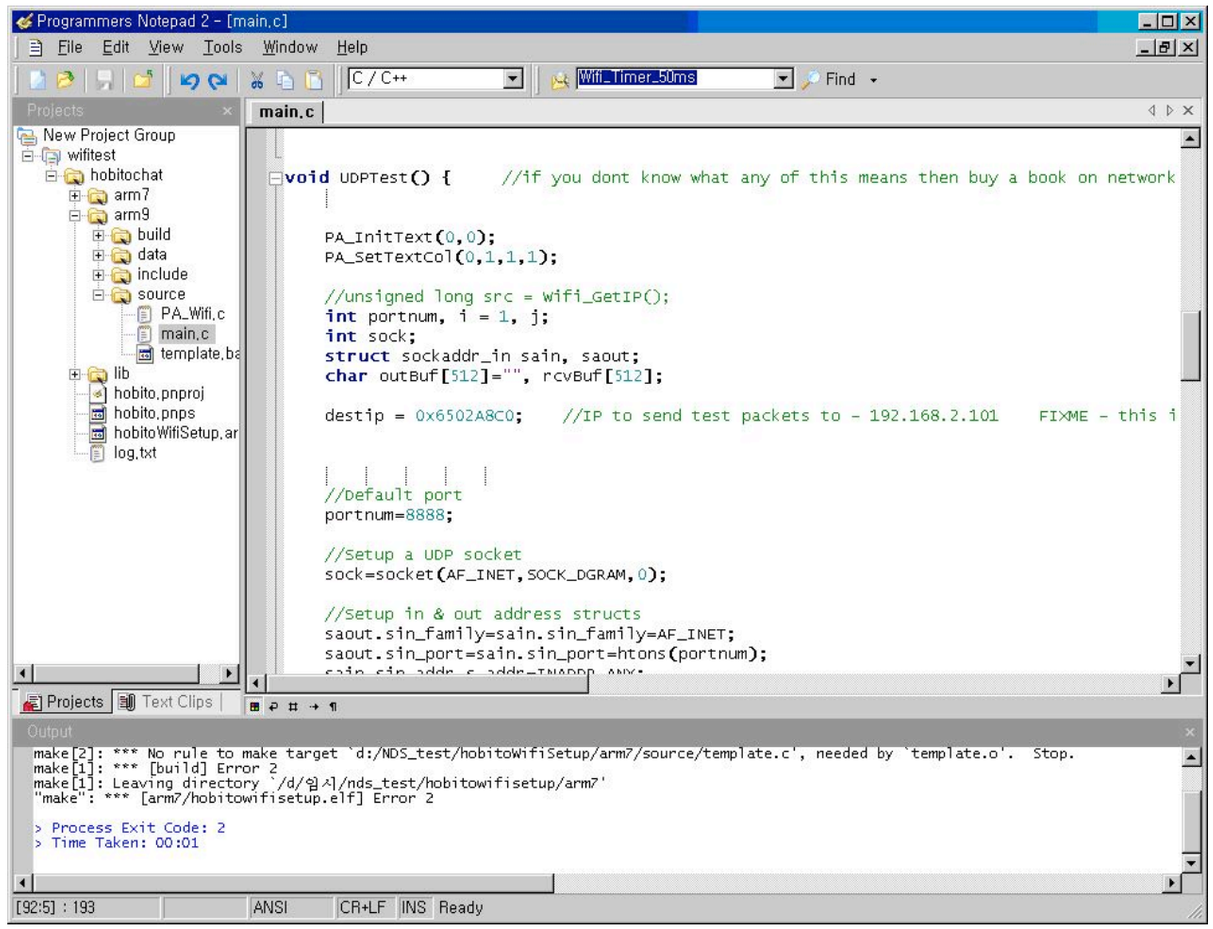
- Python Script
  NDS Python, NDS용 파이썬 해석기
  네트워크가 지원된다면 강력한 해킹 도구로 사용 가능
  http://www.disinterest.org/NDS/Python25.html

Part Two

공격용 홈브류를 만들어 사용하기

How to make homebrew

- **devkitPro**
  간단한 설치만으로 홈브류 제작에 필요한 컴파일러, 편집기 등의 도구와 설정을 완벽히 지원
  http://www.devkitpro.org/



Vortex Level 0

Vortex Level 0 문제 풀이

Remote Exploit One

Linux 시스템의 원격 취약점을 이용한 Exploit

Bind Shell 생성 후 NDS를 이용하여 접속

Remote Exploit Two

Windows 시스템의 원격 취약점을 이용한 Exploit

Win2DS 서버 설치 후 NDS를 이용하여 접속

LAN DoS Attack

One

ARP 스푸핑을 이용한 네트워크 서비스 거부 공격

호스트 ARP 캐시테이블 수정
GW의 MAC 주소를 존재하지 않는 것으로 변경

LAN DoS Attack

Two

ARP 스푸핑을 이용한 네트워크 서비스 거부 공격

GW의 ARP 캐시테이블 수정

호스트들의 MAC 주소를 존재하지 않는 것으로 변경

Part Three

예상 시나리오

공격용 홈브류의 기능 예상

- **Network Scan**
  AP, 네트워크에 존재하는 호스트, 접근 가능한 포트 스캔
- **Terminal**
  NC(Net Cat)과 비슷한 동작
- **Remote Exploit**
  원격지 시스템 취약점 공격, Shell, Remote Control 서버 설치
- **LAN DoS Attack**
  ARP 스푸핑을 이용한 서비스 거부 공격
- **Stealth**
  특정 버튼을 눌러 게임 화면으로 전환하여 공격 화면 숨김

기업 핵심 기술 유출

- 보안 검문 통과
  노트북, PDA 등의 반입을 제한하지만 NDS는 게임기라는 인식
- 사내망 접근
  편의를 위해 임의로 설치한 유무선 공유기 탐색
- 취약한 시스템 스캔
  접근 가능한 시스템의 IP 및 포트 번호
- Exploit 및 시스템 장악
  미리 제작한 여러 가지 Exploit으로 시스템의 제어권 획득
  Shell 혹은 원격 제어 프로그램을 설치하여 기밀 수집

학사 정보 조작

- 학사 관리 시스템 계정,비밀번호 수집
  교내 홈페이지 등의 취약점을 이용, 하지만 학내망에서만 접근 가능
- 학내망 접근
  공용 PC, 학교 안내 시스템 등에 장착된 USB 포트에 USB 무선 공유기 설치
  게임기라는 인식 때문에 의심 받지 않고 접근
- 학사 관리 시스템 접근
  취약한 시스템을 찾아서 Exploit하고 원격 제어 프로그램으로 학사 관리 시스템에 접속, 학사 정보 조작

행사 진행 방해

- 행사 진행을 위해 SSID, WEP Key를 공개
  ARP 스푸핑을 통한 네트워크 장애 유발
- 주최측에서 제공한 노트북만 반입 허가
  게임기라는 인식으로 NDS를 반입하여 네트워크 장애 유발
- 호스트들의 GW MAC 주소가 정적으로 설정되어 있을 경우
  GW의 캐시 테이블 변조를 통하여 네트워크 장애 유발

악성 홈브류

- 악성 홈브류 제작
  네트워크 스니핑, 네트워크 장애, 악성코드 유포 등을 포함하는 홈브류 개발
  무료 전화, 재미있는 게임 등으로 포장
- 사용자의 악성 홈브류 실행
  인터넷에 올라온 무료 전화, 재미있는 게임 홈브류를 다운 받아 NDS에서 실행
- 피해 발생
  개인 정보 유출, 네트워크 장애, 동일한 네트워크에 존재하는 시스템에 악성코드 감염 등의 피해 발생

변조된 게임 이미지

- 악성 홈브류를 불법 게임 이미지에 포함
  인터넷에 공개된 불법 게임 이미지에 악성 홈브류를 삽입
  해당 게임은 정상적으로 실행되지만 악성 홈브류도 실행 됨
- 사용자의 악성 홈브류 실행
  게임을 구입하지 않고, 불법으로 다운 받아 실행할 때 해당 이미지에 악성 홈브류가 삽입되었는지 구분할 수 없음
- 피해 발생
  개인 정보 유출, 네트워크 장애, 동일한 네트워크에 존재하는 시스템에 악성코드 감염 등의 피해 발생

Part Four

대응방안

보안 관리자

- 전자기기 반입 규정 강화
  NDS 및 휴대용 전자 기기들을 해킹 도구로 사용할 수 있음을 인지
- 비인가 AP 제거
  대부분의 휴대용 기기들은 무선랜 디바이스를 이용하여 네트워크에 접근
- 공용 PC 보안
  USB, IEEE 1394, LAN 포트 등의 사용 제한
  내부의 PC들과 네트워크 분리

NDS 사용자

- 타인의 제작한 홈브류 이용 주의
  믿을 수 있는 제작자인지 확인
  해당 홈브류가 네트워크를 사용하지 않는데 NDS에 장착된 무선랜 사용 램프가 점등 될 경우 악성 홈브류 의심
- 불법으로 다운 받은 게임 이미지 실행 주의
  정식으로 게임을 구입하여 게임을 즐겨야 함

Questions?

security@i3eat.org
http://i3eat.org/