학사학위 논문

# 사이버 보안 교육을 위한 칼리 리눅스를 활용한 윈도우 서버 침투 테스트 실습 및 환경구축 방법론

# Methods for Setting Up a Windows Server Penetration Testing Lab Environment Using Kali Linux for Cyber Security Education

2024년 12월


중부대학교

정보보호학과

정 찬 하

학사학위 논문

# 사이버 보안 교육을 위한 칼리 리눅스를 통한 윈도우 서버 침투 테스트 실습 환경구축 방법론

# Methods for Setting Up a Windows Server Penetration Testing Lab Environment Using Kali Linux for Cyber Security Education

2024년 12월


중부대학교

정보보호학과

정 찬 하

학사학위 논문

# 사이버 보안 교육을 위한 칼리 리눅스를 통한 윈도우 서버 침투 테스트 실습 환경구축 방법론

지도교수 양 환 석

이 논문을 학사학위 논문으로 제출함

2024년 12월


중부대학교

정보보호학과

정 찬 하

정 찬 하의 학사학위 논문을 인준함

심 사 위 원 장 _____ 인

심 사 위 원 _____ 인

심 사 위 원 _____ 인

2024년 12월

중부대학교

정 찬 하의 학사학위 논문을 인준함

심 사 위 원 장 _____ 인

심 사 위 원 _____ 인

심 사 위 원 _____ 인

심 사 위 원 _____ 인

심 사 위 원 _____ 인

2024년 12월

중부대학교

# 감사의 글

오랜 기간 동안 대학 생활을 잘 마무리할 수 있도록 물질적, 감정적으로
지원해 준 가족에게 감사의 말씀을 전하고, 올바른 방향성을 제시해
주신 양환석 교수님께도 감사드립니다.

**정 찬 하**

# 목 차

# 표 목 차

# 그 림 목 차

국문초록

# 사이버 보안 교육을 위한 칼리 리눅스를 통한 윈도우 서버 침투 테스트 실습 환경 구축 방법론

정찬하

정보보호 학과

중부대학교

사이버 보안 교육에서 실습 환경을 구축하는 것은 학습자들이 이론뿐만 아니라 실제적인 기술을 습득할 수 있는 필수적인 과정이다. 특히, 이터널블루(Eternal Blue) 취약점을 활용한 모의 침투 실습은 사이버 공격의 실질적인 위협을 체감하게 하고, 이를 통해 학습자들이 취약점 분석 및 공격 방어 역량을 기를 수 있는 강력한 도구이다. 그러나 현재까지의 교육 과정은 주로 이론에 치중되어 있으며, 실습 환경 구축과 공격 수행 과정을 체계적으로 다룬 자료가 부족하다는 한계가 있다.

본 논문은 다양한 모의 침투 테스트 방법과 비교하여, 이터널블루 기반의 실습 환경이 어떠한 측면에서 교육적으로 더 효과적이고, 실습자에게 실질적인 학습 경험을 제공하는지를 분석하고자 한다. 이를 위해 VulnHub 모의 침투 실습, Eternal Blue 취약점 연구, 그리고 SMB 릴레이 공격을 포함한 여러 다른 방법론을 살펴본 후, 필자가 제안하는 방식

이 기술적, 교육적 측면에서 우수함을 강조할 것이다.

특히, 필자의 연구는 VMware와 Windows Server 2012 R2 환경에서의 네트워크 설정, 취약점 스캐닝, 그리고 이터널블루 취약점을 통한 원격 제어권 획득까지의 과정을 구체적으로 제시한다. 이 과정에서 이터널블루 공격이 단순히 인증 정보를 탈취하는 SMB 릴레이 공격과 달리, 시스템 전체에 영향을 미치는 점을 학습자들이 직접 체험할 수 있다. 이러한 실습은 학습자가 보안 취약점의 심각성을 실감하고, 보안 방어 전략을 효과적으로 수립하는 데 큰 도움을 줄 수 있다.

또한, VulnHub을 통한 실습 방법과 비교했을 때, 필자의 방법론은 공격 과정을 보다 직관적이고 실질적으로 제공함으로써, 학습자들이 취약점 분석에서 공격 수행까지의 전 과정을 직접 체험할 수 있도록 돕는다. Gupta의 연구와도 비교했을 때, 필자의 방식은 보다 구체적이고 교육적이며, 학습자들이 실제 환경에서 사이버 공격에 대응하는 방법을 쉽게 이해할 수 있도록 한다. 이러한 측면에서, 본 연구는 이론적 학습에 그치지 않고 실질적인 기술 습득을 가능하게 하는 효과적인 교육 도구로서의 가치를 지닌다.

결론적으로, 본 논문은 사이버 보안 교육에서 실습 환경 구축의 중요성을 강조하며, 다른 모의 침투 방법론과 비교했을 때 필자의 방법론이 기술적, 교육적 측면에서 더 큰 효과를 낼 수 있음을 입증한다. 뿐만 아니라 실습 환경 구성과 실습을 A~Z 정밀히 기술함으로 실습 환경 구축에 어려움을 겪는 학습자들에게 구체적이고 체계적인 가이드를 제공하고, 보안 대응 능력을 향상시키는 데 실질적인 기여를 하고자 한다.

## ABSTRACT

# How to Build a Windows Server Penetration Testing Lab Environment with Cali Linux for Cybersecurity Training

JEONG, CHAN-HA
Department of Information Security
Graduate School of Joongbu University

In cybersecurity education, building a lab environment is an essential process for learners to acquire not only theoretical but also practical skills. In particular, penetration testing using the Eternal Blue vulnerability is a powerful tool for learners to experience the real threat of cyberattacks and develop their capabilities in vulnerability analysis and attack defense. However, current courses are mainly focused on theory, and there is a lack of material that systematically covers the process of building a lab environment and conducting attacks.

Compared to various penetration testing methods, this paper aims to analyze how the EternalBlue-based lab environment is more educationally effective and provides a practical learning experience for students. To do so, I will examine several different methodologies, including VulnHub penetration labs, Eternal Blue vulnerability research, and SMB relay attacks, and highlight the technical and pedagogical superiority of my proposed approach.

Specifically, my research details the process of network setup, vulnerability scanning, and remote control takeover via the Eternal Blue vulnerability in VMware and Windows Server 2012 R2 environments. Along the way, learners can experience firsthand how the EternalBlue attack affects the entire system, unlike SMB relay attacks that simply steal credentials. This exercise can help learners realize the severity of the vulnerability and effectively develop a security defense strategy.

In addition, compared to the VulnHub training method, my methodology provides a more intuitive and practical attack process, allowing learners to experience the entire process from vulnerability analysis to attack execution. Compared to Gupta's work, my methodology is more concrete and pedagogical, allowing learners to easily understand how to respond to cyberattacks in a real-world environment. In this respect, this study is valuable as

an effective teaching tool that enables practical skill acquisition rather than just theoretical learning.

In conclusion, this paper emphasizes the importance of building a lab environment in cybersecurity education and demonstrates that, compared with other penetration methodologies, our methodology has greater technical and pedagogical benefits. Furthermore, by providing an A-Z description of the lab environment configuration and exercises, we hope to provide a concrete and systematic guide for learners who have difficulties in building a lab environment and make a practical contribution to improving their security response capabilities.

# 제 1 장 서 론

## 1.1 연구의 배경

사이버 보안 교육에서 실습 환경 구축의 중요성은 점점 더 부각되고 있다. 이론적인 지식만으로는 실제 사이버 공격과 방어 기술을 충분히 이해하고 습득하기 어려우며, 이러한 한계를 극복하기 위해서는 실제 환경에서의 실습이 필수적이다. 특히, 이론만으로는 체득하기 어려운 네트워크 공격과 취약점 악용에 대한 구체적인 경험을 제공하기 위해, 실습 환경에서의 도전적인 실제 사이버 보안 시뮬레이션이 필요하다. Luay A. Wahsheh와 Biruk Mekonnen의 연구에서도, 튜토리얼 실습이 학습자들의 문제 해결 능력을 향상시키고 실질적인 보안 지식을 제공하는 데 중요한 역할을 한다고 강조한 바 있다.[1)]

하지만 실제로 실습 환경을 구축하는 것은 학습자들에게 큰 도전 과제이다. 필자는 실습 환경을 체계적으로 구축하는 과정에서 다양한 조각난 정보를 수집하고 연결하는 데 많은 어려움을 겪었다. 이에 따라 본 논문은 A부터 Z까지 실습 환경을 체계적으로 구축하는 방법을 상세히 제시하며, 특히 이터널블루 공격을 활용한 모의 침투 실습이 다른 모의 침투 방법들과 비교했을 때, 교육적으로 가장 효과적인 방법임을 논의하고자 한다. 이를 통해 사이버 보안 실습 환경을 체계적으로 구성하려는 학습자들에게 구체적인 지침을 제공하고, 다른 방법들과의 비교를 통해 필자의 방법론이 더욱 효과적임을 입증할 것이다.

---

1) Luay A. Wahsheh, Biruk Mekonnen, "Practical Cyber Security Training Exercises," presented at the IEEE Computer Society Conference on Cybersecurity, 2019, pp. 48.

## 1.2 연구의 목적

본 논문의 목적은 다양한 모의 침투 테스트 방식 중에서 이터널블루 기반 실습 환경 구축 방법을 단계별로 자세히 설명하고, 그 과정에서 고려해야 할 기술적 요구 사항을 명확히 제시하는 것이다. 이를 통해 학습자들은 실제 보안 실습 환경을 구축하는 데 필요한 구체적인 지식을 습득할 수 있을 것이다. 특히, 본 연구는 이터널블루 공격을 활용한 윈도우 서버의 권한 획득 시나리오를 중심으로, 필자의 경험을 바탕으로 실습 환경 구축의 실제적인 어려움과 그 해결 방안을 논의할 것이다. 또한 이터널블루 실습 방법이 다른 모의 침투 방식에 비해 어떤 점에서 더 효율적이고 교육적으로 유용한지 비교하여 설명할 것이다.

## 1.3 연구 필요성

사이버 보안 교육에서 실습 환경을 효과적으로 구축하는 것은 이론뿐만 아니라 실제적인 기술을 습득할 수 있는 기회를 제공하는 데 중요한 역할을 한다. 예를 들어, 이터널블루 취약점 공격을 위한 환경구축을 직접 구축하며 실습하는 것은 학생들이 단순한 이론적 학습을 넘어서, 실제 시스템의 취약점을 이해하고 이를 악용하는 방법을 직접 경험할 수 있게 한다. 이는 학습자들이 보안 취약점에 대한 깊이 있는 이해를 돕고, 나아가 실제 사이버 공격에 대응할 수 있는 능력을 기르는 데 중요한 역할을 한다. 본 논문에서는 이와 같은 실습이 다른 모의 침투 방식과 비교했을 때 교육적 가치가 더 크다는 점을 강조하고, 이를 뒷받침하는 다양한 실험 결과와 분석을 제시할 것이다.

## 1.4 논문 구성

본 논문은 총 네 개 장으로 구성되어 있으며, 각 장은 다음과 같은 내용을 포함하고 있다.

제 1 장 서론에서는 연구의 배경과 목적, 필요성을 설명하고, 본 논문의 전체적인 구성에 대해 간략히 소개한다.

제 2 장 이론적 배경에서는 사이버 공격의 개요를 다루며, 다양한 공격의 종류와 목표, 그리고 취약점 및 공격 벡터에 대한 정의와 사례를 제시한다. 특히 이터널블루(Eternal Blue) 공격의 원리와 관련된 악용 사례를 통해 이론적 이해를 높인다. 또한 관련 연구를 소개한다 SMB 프로토콜의 취약점을 활용한 다른 모의 침투 테스트 방법론들을 제시하고, 필자의 방법론과 비교 분석한다. 이 과정에서 두 방법론 간의 차이점과 필자의 방법론이 가지는 효과성과 교육적 가치를 강조하여, 사이버 보안 교육에서의 실습 환경 구축의 중요성을 부각시킨다.

제 3 장 환경 구축 및 실습에서는 VMware Workstation Pro와 Kali Linux, Windows Server 2012 R2의 설치 과정을 상세히 설명하고, 모의 침투 실습을 위한 환경을 구성하는 방법을 안내한다. 이를 통해 실제 사이버 공격 시나리오를 체험할 수 있도록 돕는다.

제 4 장 결론에서는 연구 결과를 요약하고, 향후 연구 계획에 대한 제안을 포함한다. 이 장에서는 본 연구가 사이버 보안 교육 분야에 미치는 기여와 함께, 추가적인 연구 방향을 제시할 예정이다.

# 제 2 장 이론적 배경

## 2.1 사이버 공격의 개요

사이버 공격은 네트워크, 컴퓨터 시스템 또는 디지털 장비에 무단으로 접근하여 데이터, 애플리케이션 또는 기타 자산을 도용, 노출, 변경, 비활성화하거나 파괴하는 의도적인 행위를 의미한다. 이러한 공격은 다양한 동기에서 발생하며, 위협 행위자는 사소한 절도에서부터 국가 간 사이버 전쟁에 이르기까지 폭넓은 목적을 가지고 활동한다. 사이버 공격은 개인, 기업, 정부 기관을 막론하고 심각한 피해를 초래할 수 있으며, 그 영향은 경제적 손실뿐만 아니라 신뢰도 및 평판에도 큰 영향을 미친다.

위협 행위자들은 악성 코드 공격, 소셜 엔지니어링 사기, 비밀번호 도용 등의 다양한 전술을 통해 표적 시스템에 접근한다. 이러한 공격은 조직의 비즈니스를 방해하거나 심지어 파괴할 수 있다. 특히 데이터 침해의 경우, 이를 복구하는 데 드는 평균 비용은 약 435만 달러에 이르며, 이는 위반을 발견하고 대응하는 비용, 다운타임, 매출 손실, 그리고 장기적인 브랜드 평판 손상 등을 모두 포함한 금액이다.

일부 사이버 공격은 그 피해가 더욱 심각할 수 있다. 예를 들어, 랜섬웨어 공격의 경우 피해 기업에 최대 4천만 달러를 요구하기도 하며, 비즈니스 이메일 침해(BEC) 사기는 단 하나의 공격으로도 피해자에게 4천 7백만 달러에 달하는 손실을 초래할 수 있다. 또한, 고객의 개인 식별 정보(PII)를 훼손하는 공격은 고객의 신뢰를 무너뜨릴 뿐만 아니라 규제 벌금 및 법적 조치로 이어질 수 있다. 한 추산에 따르면, 사이버 범죄로 인한 세계 경제의 연간 비용은 2025년까지 10조 5천억 달러에 이를 것

으로 예상된다. 또한 국내에서는 업 규모별 침해사고의 경제적 피해액은 대기업(20.9억원), 중견기업(17.4억), 중소기업(4.4억원), 비영리재단(0.2억원) 순으로 기업규모가 클수록 커지는 것으로 조사되었다.[2)]

따라서 사이버 공격의 유형과 주요 특징을 이해하는 것은 사이버 보안 방어 전략을 수립하는 데 필수적이다. 본 장에서는 사이버 공격의 정의와 그로 인해 발생할 수 있는 잠재적 위협을 고찰하며, 이러한 공격이 조직에 미치는 영향을 논의한다.

### 2.1.1 사이버 공격의 종류

사이버 공격은 여러 유형으로 분류될 수 있으며, 이들은 공격의 목표, 방법, 그리고 의도에 따라 다르다. 각 유형의 사이버 공격은 특정한 기술적 수단을 쓰며, 다양한 수준의 피해를 초래할 수 있다. 본 절에서는 사이버 공격을 물리적 공격, 네트워크 공격, 응용 프로그램 공격으로 구분하여 설명한다.

2) 이용필, 김태성, 유진호, "국내 사이버 침해사고의 경제적 피해 금액 산정," Korea Business Review, 24(2) (2020): 1.

#### 2.1.1.1 물리적 공격

물리적 공격은 네트워크나 시스템의 하드웨어 장비에 직접적으로 영향을 미치는 공격을 의미한다. 이러한 공격은 보통 물리적 접근을 통해 이루어지며, 장비의 손상, 데이터의 도난, 또는 시스템의 파괴를 초래할 수 있다. 예를 들어, 데이터 센터의 하드 드라이브를 물리적으로 훼손하거나, 네트워크 케이블을 절단하는 등의 행위가 물리적 공격에 해당한다. 이러한 공격은 보안 시스템의 물리적 취약점을 악용하며, 그 결과로 시스템 전체의 기능을 마비시키는 경우가 많다.

#### 2.1.1.2 네트워크 공격

네트워크 공격은 조직의 네트워크 인프라를 대상으로 하는 공격으로, 네트워크의 취약점을 이용하여 불법적인 접근, 데이터 탈취, 서비스 방해 등을 시도한다. 네트워크 공격은 주로 분산 서비스 거부(DDoS) 공격, 스푸핑, 중간자 공격(MITM), 그리고 침입 시도와 같은 형태로 나타난다. 이러한 공격은 네트워크 트래픽을 방해하거나, 민감한 데이터를 탈취함으로써 조직의 운영에 큰 혼란을 초래할 수 있다. 네트워크 공격은 특히 원격 근무의 확산과 함께 그 빈도와 복잡성이 증가하고 있다.

#### 2.1.1.3 응용 프로그램 공격

응용 프로그램 공격은 소프트웨어 애플리케이션의 취약점을 목표로 하는 공격이다. 이러한 공격은 애플리케이션에 존재하는 버그나 설정 오류를 이용해 비정상적인 동작을 유도하거나, 데이터를 무단으로 수정, 삭제, 또는 탈취하려는 시도를 포함한다. 예를 들어, SQL 인젝션, 크로스 사이트 스크립팅(XSS), 버퍼 오버플로우 등의 공격이 대표적이다. 응용 프로그램 공격은 보통 사용자가 자주 접속하는 웹사이트나 애플리케이션을

목표로 하며, 그 결과로 개인 정보 유출, 시스템 침해, 서비스 장애 등을 초래할 수 있다.

이처럼 다양한 사이버 공격의 종류는 조직의 보안 전략 수립에 있어서 중요한 고려 사항이 된다. 각 공격 유형에 대한 이해를 바탕으로 적절한 방어 체계를 마련하는 것이 중요하다.

### 2.1.2 사이버 공격의 목표

사이버 공격의 주요 목표는 여러 가지로 분류될 수 있다. 첫째, 정보 탈취는 공격자가 민감한 정보나 데이터를 불법적으로 획득하기 위해 이루어지는 행위로, 개인 식별 정보(PII), 기업의 상업 비밀, 국가의 기밀 데이터 등이 대상이 된다. 이러한 정보는 주로 재정적 이득을 위해 탈취되며, 이후 판매되거나 악용될 가능성이 크다.

둘째, 시스템 손상은 공격자가 악성 소프트웨어를 이용하여 시스템의 정상적인 운영을 방해하거나 접근 권한을 차단하는 방식으로 이루어진다. 이는 시스템의 기능을 마비시키고, 결과적으로 기업이나 기관의 운영에 심각한 영향을 미칠 수 있다.

셋째, 서비스 중단을 목표로 하는 공격은 주로 서비스 거부 공격(DoS) 또는 분산 서비스 거부 공격(DDoS) 형태로 나타나며, 웹사이트나 네트워크 서비스의 정상적인 이용을 방해하는 데 초점을 맞춘다. 이는 기업의 운영에 큰 피해를 주며, 사용자 신뢰도에 부정적인 영향을 미칠 수 있다.

넷째, 금전적 이득을 목표로 하는 공격은 랜섬웨어 공격이나 비즈니스 이메일 침해(BEC) 사기와 같이 피해자에게 금전을 요구하거나 기업의 재정 자원을 직접적으로 탈취하는 형태로 나타난다. 이러한 공격은 피해

기업에 상당한 재정적 손실을 초래한다.
마지막으로, 정치적 또는 사회적 목표를 달성하기 위해 사이버 공격이 수행되기도 한다. 국가 간의 사이버 전쟁이나 사이버 테러는 정치적 이득을 취하거나 사회적 혼란을 초래하기 위해 이루어지며, 이러한 공격은 주로 정부 기관이나 사회적 중요한 인프라를 대상으로 한다.
사이버 공격의 형태와 목표는 다양하며, 이에 따라 각기 다른 방어 전략이 요구된다. 이러한 공격에 대한 적절한 대응 및 예방 조치를 마련하는 것은 조직의 필수적인 과제로 인식된다.

## 2.2 취약점과 공격 벡터

사이버 보안에서 취약점과 공격 벡터는 매우 중요한 개념으로, 시스템과 네트워크의 보안을 평가하고 보호하기 위해 필수적으로 이해해야 한다. 취약점은 시스템, 소프트웨어, 네트워크 또는 기타 디지털 자산 내에서 악용될 수 있는 결함이나 허점이다. 반면, 공격 벡터는 공격자가 이러한 취약점을 이용해 시스템에 접근하고 공격을 수행하는 방법이나 경로를 의미한다. 취약점과 공격 벡터의 상호작용은 사이버 공격의 성공 여부를 결정짓는 중요한 요소이며, 효과적인 보안 전략을 수립하기 위해서는 이들 간의 관계를 깊이 이해해야 한다.

### 2.2.1 취약점의 정의와 종류

취약점은 소프트웨어, 하드웨어, 네트워크 구성 요소, 또는 인간적 요소에서 발생할 수 있는 약점이나 결함으로 정의된다. 이러한 취약점은 시스템의 보안을 저해하며, 공격자가 시스템에 무단 접근할 기회를 제공한다. 취약점은 다양한 형태로 나타나며, 주요 종류는 다음과 같다.
첫째, 소프트웨어 취약점은 버그, 프로그래밍 오류, 잘못된 설정 등 소프

트웨어에서 발견되는 결함을 의미한다. 예를 들어, 버퍼 오버플로우(Buffer Overflow)와 같은 취약점은 공격자가 악성 코드를 실행하거나 시스템을 장악할 수 있는 기회를 제공한다.

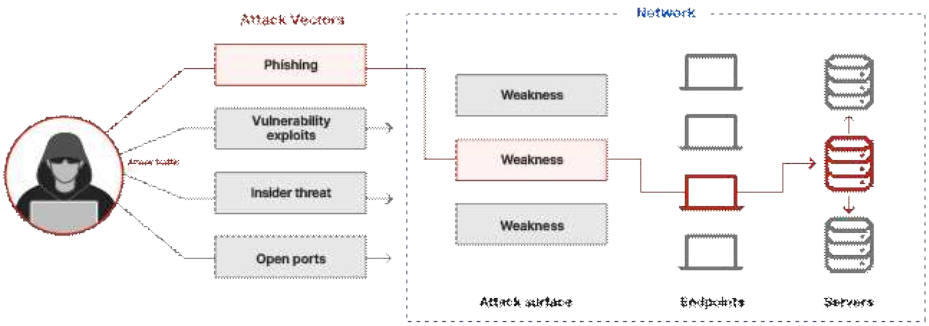
둘째, 하드웨어 취약점은 하드웨어 설계나 구현 과정에서 발생하는 결함을 의미한다. 이는 하드웨어의 물리적 결함이나 펌웨어의 취약성으로 나타날 수 있다. 예를 들어, 사이드 채널 공격(Side Channel Attack)은 하드웨어의 취약점을 악용하는 대표적인 사례이다.

셋째, 네트워크 취약점은 네트워크 프로토콜, 구성, 또는 구현 과정에서 발견되는 결함을 의미한다. 이러한 취약점은 공격자가 네트워크를 가로채거나 침입할 수 있는 기회를 제공한다. 미스코디네이션된 방화벽 규칙이나 보안 설정의 부재는 네트워크 취약점을 초래할 수 있는 예시이다.

마지막으로, 인간적 취약점은 사용자나 관리자의 실수, 잘못된 판단, 또는 부주의로 인해 발생하는 취약점을 의미한다. 이는 소셜 엔지니어링(Social Engineering)과 같은 공격이 성공할 수 있는 주요 요인 중 하나로 작용한다.

이러한 취약점은 시간이 지나면서 발견되고 수정되지만, 새로운 취약점도 계속해서 등장하므로 보안 담당자들은 지속해서 시스템을 업데이트하고 취약점을 관리해야 한다.

### 2.2.2 공격 백터의 개념




[그림 2-1] 공격 벡터

공격 벡터(Attack Vector)는 사이버 공격자가 네트워크, 시스템, 또는 애플리케이션에 침투하기 위해 사용하는 경로나 수단을 의미한다. 이는 공격자가 취약점을 악용하여 시스템에 접근하고, 정보를 탈취하거나 시스템을 훼손하는 과정에서 사용하는 다양한 방법론을 포함한다. 사이버 보안에서 공격 벡터를 이해하는 것은 잠재적인 위협을 예측하고 방어 체계를 강화하는 데 필수적이다.

공격 벡터는 물리적 접근, 소프트웨어 취약점의 악용, 소셜 엔지니어링과 같은 다양한 형태로 나타날 수 있으며, 그 종류에 따라 다르게 대응해야 한다. 예를 들어, 피싱 공격은 사용자의 비밀번호와 같은 민감한 정보를 탈취하기 위해 피해자를 속이는 소셜 엔지니어링의 일종이다. 이와 같은 피싱 공격은 랜섬웨어와 같은 악성 프로그램의 배포를 위해 자주 사용되며, 여전히 가장 일반적인 공격 벡터 중 하나로 꼽힌다.

또한, 이메일 첨부 파일은 사용자가 열 때 악성 코드를 실행하는 악성 프로그램을 포함할 수 있는 또 다른 일반적인 공격 벡터이다. 이는 공격자가 네트워크 내에서 권한을 획득하고, 시스템에 심각한 손상을 입히는

데 사용된다. 계정 탈취 역시 중요한 공격 벡터로, 공격자는 무차별 대입 공격 또는 피싱을 통해 사용자 자격 증명을 탈취하여 시스템에 침입할 수 있다.

암호화되지 않은 데이터 전송은 네트워크상에서 쉽게 가로챌 수 있는 공격 벡터를 제공하며, 이에 따라 민감한 데이터가 유출될 위험이 있다. 내부자 위협은 조직 내부의 사용자가 고의적으로 또는 우발적으로 기밀 정보를 유출하는 경우를 말하며, 이는 외부 공격자에게 큰 기회를 제공할 수 있다.

마지막으로, 취약점 익스플로잇은 소프트웨어 또는 하드웨어의 결함을 이용하여 공격자가 시스템에 침입하는 것을 의미한다. 이는 제로데이 취약점과 같은 수정되지 않은 결함을 통해 발생할 수 있으며, 브라우저 기반의 공격이나 애플리케이션 손상과 같은 여러 경로를 통해 악용될 수 있다.

이처럼 공격 벡터는 매우 다양하며, 이를 차단하기 위해서는 강력한 보안 관행과 체계적인 방어 전략이 요구된다. 각 공격 벡터에 대한 철저한 이해와 대응책 마련이 사이버 보안의 핵심이라 할 수 있다.

### 2.2.3 일반적인 취약점 사례

사이버 공격의 주요 원인 중 하나는 시스템의 취약점에 있다. 취약점은 시스템, 소프트웨어, 또는 하드웨어의 약점으로, 공격자가 이를 악용하여 시스템에 무단으로 접근하거나 손상을 입힐 수 있다. 일반적인 취약점 사례로는 피싱, 이메일 첨부 파일, 계정 탈취, 암호화 부족, 내부자 위협, 취약점 익스플로잇, 브라우저 기반 공격, 애플리케이션 손상, 그리고 열린 포트가 있다.

피싱은 가장 흔한 취약점 중 하나로, 사용자를 속여 중요한 정보를 도용

하는 공격 기법이다. 공격자는 주로 이메일, 문자 메시지, 또는 웹사이트를 통해 피해자가 민감한 정보를 제공하도록 유도하며, 이는 많은 랜섬웨어 공격의 출발점이 된다.

이메일 첨부 파일 역시 자주 이용되는 취약점으로, 사용자가 파일을 열 때 악성 코드가 실행되어 시스템을 감염시킬 수 있다. 최근 몇 년간 Ryuk과 같은 주요 랜섬웨어 공격이 이 방법을 통해 이루어졌다.

계정 탈취는 공격자가 합법적인 사용자 계정을 무단으로 획득하는 방식으로, 피싱 공격, 무차별 대입 공격, 또는 지하 시장에서 자격 증명을 구매하는 등의 방법으로 이루어진다. 또한, 공격자는 세션 쿠키를 가로채어 사용자로 가장할 수 있다.

암호화가 부족한 경우, 네트워크를 통해 전송되는 데이터가 쉽게 가로채질 수 있는 취약점을 제공한다. 이러한 취약점은 경로상 공격을 통해 민감한 정보가 도용되는 결과를 초래할 수 있다.

내부자 위협은 시스템 내부의 사용자에 의해 발생할 수 있는 취약점으로, 악의적인 내부자가 고의로 또는 실수로 기밀 정보를 유출하거나, 외부 공격자가 내부자를 매수 또는 협박하여 발생할 수 있다.

취약점 익스플로잇은 시스템 또는 소프트웨어의 결함을 이용한 공격으로, 공격자가 이러한 취약점을 통해 시스템에 접근할 수 있다. 이는 보안 업데이트를 적용하지 않았으면 특히 노출되기 쉽다.

브라우저 기반 공격은 웹 페이지를 표시하기 위해 원격 서버에서 받은 코드를 로드하고 실행하는 과정에서 발생하는 취약점이다. 공격자는 악성 코드를 삽입한 웹사이트를 통해 사용자의 브라우저를 감염시켜, 시스템에 맬웨어를 다운로드하거나 실행할 수 있다.

애플리케이션 손상은 신뢰할 수 있는 타사 애플리케이션을 맬웨어로 감염시키거나, 사용자가 무의식적으로 다운로드하여 설치하는 가짜 애플리

케이션을 통해 시스템에 침투할 수 있는 취약점이다.
마지막으로, 열린 포트는 네트워크 트래픽을 통해 시스템에 침투할 수 있는 취약점을 제공한다. 공격자는 특정 메시지를 열린 포트에 보내 시스템을 손상시키려 시도할 수 있으며, 이에 따라 사용하지 않는 포트를 닫는 것이 중요하다.
이와 같은 일반적인 취약점 사례들은 보안 관리와 정책에서 중요한 고려사항으로 작용하며, 이를 통해 조직의 정보 보안을 강화할 수 있다. 본 논문에서 다루는 이터널블루 공격은 이러한 취약점 중 취약점 익스플로잇에 속하며, Windows Server 2012 R2 운영체제의 SMB 프로토콜 취약점을 이용하여 이루어지는 공격이다.

## 2.3 이터널블루(Eternal Blue) 공격 개요

### 2.3.1 이터널 블루의 정의와 개요

이터널블루(EternalBlue)는 미국 국가안보국(NSA)이 개발한 해킹 툴로, 2016년 8월 쉐도우 브로커스(Shadow Brokers)라는 해커 그룹에 의해 유출되었다. 이 도구는 Microsoft Windows 운영체제에서 SMB(Server Message Block) 프로토콜의 취약점을 이용하여 원격 코드 실행이 가능하도록 설계되었다. 이터널블루는 사이버 범죄자들에 의해 악용되었으며, 특히 워너크라이(WannaCry) 랜섬웨어와 낫페트야(NotPetya) 공격에서 중요한 역할을 하였다.

### 2.3.2 이터널블루 공격의 원리

이터널블루(EternalBlue)는 SMB 프로토콜에서 발견된 취약점을 악용하여 원격으로 시스템을 침투할 수 있다. SMB 프로토콜은 Windows 운영

체제에서 파일 공유, 프린터 공유 및 원격 서비스 접근을 위해 사용되며, 주로 TCP 포트 139와 445에서 운영된다. 이터널블루 공격은 SMB 버전 1과 TCP 포트 445를 통해 이루어지며, 공격자는 이 취약점을 통해 악성 코드를 로드하고, 네트워크 내의 다른 시스템으로 확산시킬 수 있다.

공격은 먼저 SMB 클라이언트와 서버 간의 초기 핸드셰이크를 통해 시작된다. 이후 공격자는 잘못된 Secondary Trans2 요청을 이용하여 취약점을 트리거한다. 이 과정에서 srv2.sys 커널 드라이버의 취약점을 악용하여 시스템에 악성 코드를 실행하게 된다.

### 2.3.3 이터널블루와 관련된 보안 취약점

이터널블루(EternalBlue)는 Microsoft Windows 운영체제의 SMB 프로토콜에서 발생한 심각한 보안 취약점을 기반으로 한다.[3] 이 취약점은 Microsoft의 보안 공지 MS17-010에 명시되어 있으며, 시스템에서 버퍼 오버플로우를 유발하여 악성 코드가 실행될 수 있는 위험을 내포하고 있다. 이러한 취약점은 패치되지 않은 시스템에 큰 위협이 되었으며, 이에 따라 워너크라이 랜섬웨어와 같은 대규모 사이버 공격이 발생하게 되었다.

---

3) H. Eck, "Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection," 2021 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 2021, pp. 87-92, doi: 10.1109/ISCTURKEY53027.2021.9654331.
https://ieeexplore.ieee.org/document/9654331

## 2.4 관련 연구

### 2.4.1 VulnHub을 이용한 모의침투 테스트

VulnHub의 Basic Pentesting 2를 이용한 침투 테스트 실습,

본 연구에서는 VulnHub에서 제공하는 취약한 시스템인 "Basic Pentesting 2"의 SMB 서비스 취약점을 활용하여 침투 테스트를 진행한다. 이 실습의 첫 단계로, 동일 네트워크 대역에서 연결된 호스트를 식별하기 위해 netdiscover를 사용하였고, 41번 호스트가 공격 대상 IP로 확인되었다. 이후 nmap을 통해 추가 정보를 수집한 결과, 22, 80, 139, 445, 8080, 8089 포트가 열려 있음을 확인하였다. 이 중에서 SMB 서비스가 활성화되어 있었고, 익명 계정으로 접근할 수 있는 취약점이 발견되었다.

추가적인 정보 수집 과정에서는 검색 도구인 searchsploit을 통해 관련 공격 코드를 검색했으나 특별한 결과를 찾지 못했다. 대 신, 웹 서비스에 접근하여 웹 서버의 상태를 점검한 결과, 아파치 톰캣이 운영 중임을 확인하였다. 이후 nikto를 사용해 점검하였고, 디렉터리 인덱싱 취약점이 존재함을 발견하여 두 개의 텍스트 파일을 통해 내부 정보를 수집하였다. 이 파일들에서 서버 설정과 관련된 유용한 정보를 얻었고, 특히 사용자의 비밀번호 정책이 미흡함을 알게 되었다.

SMB 취약점을 확인하기 위해 nmap의 NSE 스크립트를 이용하였으며, 익명 계정이 read와 write 권한을 가진 공유 디렉터리가 존재함을 확인하였다. 하지만, 관련 공격 모듈의 사용은 불가능한 것으로 판명되었다. 이후 enum4linux를 활용하여 사용자 계정 정보를 수집하였고, kay와

jan 두 사용자의 계정이 존재함을 확인했다. jan 계정으로 SSH에 성공적으로 접근한 후, 내부 정보를 조사하는 과정에서 kay의 디렉터리에 중요한 파일이 존재함을 발견하였다.

권한 상승 단계에서는 jan 사용자가 sudo 권한을 부여받지 못했으나, python 기반의 스크립트를 통해 특정 파일의 권한을 상승시키는 방법을 찾아내었다. 이를 통해 최종적으로 root 권한을 획득하는 데 성공하였다.

본 연구에서 적용한 방법은 Windows Server 2012 R2를 직접 설치하고 구성하는 것으로 시작한다. 이러한 접근 방식은 사용자가 시스템의 내부 구조와 운영에 대한 깊은 이해를 가능하게 한다. 반면, VulnHub의 Basic Pentesting 2 환경에서는 미리 설정된 시스템이 제공되므로, 사용자가 직접 환경을 구축하는 과정에서 얻는 학습 기회는 제한적이다.

직접 환경을 구성함으로써 사용자는 취약점의 작동 원리를 명확히 이해하고, 이를 통해 발생할 수 있는 다양한 보안 문제를 해결하는 능력을 기를 수 있다. 예를 들어, 직접 SMB 취약점을 설정하고 관리함으로써 보안 기술에 대한 실무 경험을 쌓을 수 있는 기회를 갖게 된다. 이는 단순히 미리 구성된 환경에서 실습하는 것보다 더 많은 실용적 지식을 제공한다.

또한, 자신의 필요에 맞게 환경을 조정할 수 있다는 점에서, 본 연구의 방법은 특정 공격 기법이나 시나리오를 심화 연구하는 데 유리하다. VulnHub 환경에서는 특정한 공격 벡터에 대한 실습이 제한적일 수 있지만, 사용자가 직접 구축한 환경에서는 다양한 시나리오를 실험하고 연구할 수 있다.

결론적으로, VulnHub의 접근 방식은 기본적인 기술을 익히는 데 유용할 수 있으나, 본 연구에서 제시한 방법은 더 깊이 있는 이해와 실무 경험

을 쌓는 데 기여할 것으로 기대된다. 이러한 차별화된 점은 본 연구의 방법이 교육적이고 효율적이라는 주장을 뒷받침한다.

### 2.4.2 Gupta, Manoj R., et al. "Eternal Blue Vulnerability."

본 연구에서는 EternalBlue 취약점을 활용한 Windows Server 2012 R2 환경에서의 모의 침투 테스트를 진행하였으며, 이를 통해 실습 환경 구축의 중요성을 강조하였다. 이와 관련하여 **Gupta et al.**의 연구[4]는 EternalBlue 취약점이 포함된 사이버 공격의 탐지와 완화 방법에 중점을 두고 있다. 두 연구는 동일한 취약점을 다루고 있으나, 연구의 목적과 접근 방식에서 차이가 존재한다.

Gupta 등의 논문은 EternalBlue 취약점이 야기한 사이버 공격, 특히 2017년 발생한 WannaCry 랜섬웨어 공격에 대한 탐지와 대응 방법을 제시하고 있다. 이 연구는 Microsoft의 SMBv1 취약점을 악용한 공격을 설명하고, 공격 이후의 탐지 및 방어 전략을 제안하는 데 초점을 맞춘다. 해당 연구에서는 Windows 이벤트 로그 분석과 같은 도구를 통해 취약점을 탐지하는 방법을 제시하며, 취약점 완화를 위한 보안 패치 적용, SMBv1 비활성화 등의 방법론을 강조하고 있다.

반면, 본 연구는 침투 테스트 환경 구축 및 실습 중심의 학습을 목표로 한다. 특히, Kali Linux와 Metasploit을 활용하여 Windows Server 2012 R2의 SMB 취약점을 직접적으로 익스플로잇하고, 이를 통해 meterpreter 세션을 획득하는 과정을 다루고 있다. 이 과정에서 사용자는 공격자의 관점에서 취약점을 분석하고 실습함으로써 공격 및 방어 체계 전반에 대한 실질적인 이해를 얻을 수 있다.

Gupta 등의 연구와 비교하여, 본 연구의 차별점은 공격자의 입장에서

---

4) Gupta, M. R., Koli, Y. P., Patiyane, V. A., & Wagh, K. P. Eternal Blue Vulnerability.

시스템을 분석하고 공격을 수행하는 실습 과정에 있다. Gupta 등의 연구는 취약점이 이미 악용된 상태에서 이를 탐지하고 대응하는 방어적 접근을 중심으로 하지만, 본 연구는 침투 테스트와 환경 구축을 통해 실제 공격 과정 자체를 학습하도록 한다. 이는 단순히 취약점 탐지에 머무르지 않고, 학생들이 실제로 공격 과정을 체험함으로써 사이버 보안 전반에 대한 깊이 있는 학습을 할 수 있는 기회를 제공한다.

본 연구가 교육적 측면에서 더 효과적임을 주장할 수 있는 이유는 다음과 같다. 첫째, 실습 기반의 학습을 통해 학생들은 단순한 이론적 지식을 넘어서 실제 공격 및 방어 시나리오를 경험할 수 있다. 둘째, 직접적인 환경 구성과 침투 과정을 수행함으로써 학생들은 문제 해결 능력을 기르게 된다. 예를 들어, 침투 과정에서 발생하는 네트워크 구성 문제나 익스플로잇 오류를 해결하는 과정에서 실질적인 보안 실무 능력을 키울 수 있다. 반면, Gupta 등의 연구는 공격 이후의 탐지와 대응 방법을 중점적으로 다루기 때문에 실습적인 관점에서 다소 제한적이다.

결론적으로, Gupta 등의 연구는 탐지 및 방어적 측면에서 매우 유용한 정보를 제공하지만, 본 연구는 이를 보완하여 실제 공격 과정을 중심으로 한 실습 환경을 구축하고 이를 통해 학습자의 공격적 사고와 방어적 사고를 동시에 길러준다. 이러한 방식은 특히 사이버 보안 실습 교육에서 효과적인 방법론으로 작용할 수 있다.

### 2.4.3 SMB 릴레이 공격

SMB 릴레이 공격은 SMB 프로토콜을 통해 이루어지는 대표적인 인증 위협 공격 기법 중 하나로, 공격자는 네트워크 상에서 인증 요청을 가로채어 해당 인증을 악용하여 목표 시스템에 접근할 수 있다. 이러한 SMB 릴레이 공격 방식은 주로 네트워크 내에서 동작하며, 공격자는 인증 과정에서 취약점을 발견하고 이를 이용해 네트워크 자산에 무단으로 접근하게 된다. 논문에서는 SMB 서비스가 제공하는 취약점을 구체적으로 분석하며, 이를 바탕으로 공격자가 인증을 가로채거나 시스템 내부의 중요한 데이터에 접근할 수 있는 시나리오를 소개하고 있다. 이와 같은 공격은 사용자 인증 정보의 탈취뿐만 아니라, 네트워크 내부에서의 지속적인 침투를 가능하게 한다는 점에서 심각한 보안 위협으로 간주된다.

논문에서는 또한 SMB 릴레이 공격의 수행 절차를 단계별로 상세히 설명한다. 공격자는 먼저 네트워크 환경에서 인증 정보를 수집한 후, 해당 정보를 릴레이하여 인증이 완료된 것처럼 위장한다. 이를 통해 공격자는 추가적인 시스템 자산에 접근하거나, 네트워크 상의 다른 시스템에 대한 공격을 확장할 수 있다. 이 과정에서 중요한 포인트는 SMB가 네트워크 내에서 파일 및 프린터를 공유하는 과정에서 발생하는 인증 요청을 가로챌 수 있다는 점이다. 이러한 SMB 릴레이 공격의 대표적인 사례로는 Active Directory와 같은 네트워크 인증 시스템을 겨냥한 공격을 들 수 있으며, 이를 통해 공격자는 네트워크의 다양한 자산을 무단으로 사용하거나, 인증된 사용자로 위장하여 네트워크 상의 권한을 탈취할 수 있다.

반면, 내가 수행한 이터널블루(EternalBlue) 기반의 모의 침투 실습은 SMB 프로토콜의 취약점을 활용하되, 더 직접적이고 공격적인 방식으로 진행된다. 이터널블루 공격은 MS17-010 취약점을 악용하여 원격에서 코드 실행을 가능하게 하며, 이를 통해 시스템의 제어권을 획득할 수 있

다. 특히 이 공격은 사용자 개입 없이도 자동으로 시스템에 악성 코드를 주입할 수 있다는 점에서 SMB 릴레이와는 다른 방식의 공격이다. SMB 릴레이가 인증을 위주로 하는 공격이라면, 이터널블루는 시스템 제어권 자체를 가져오는 데 초점을 맞추고 있다. 이를 통해 공격자는 시스템의 관리자 권한을 획득하고, 네트워크 상의 다른 시스템에까지 공격을 확장할 수 있게 된다.

SMB 릴레이와 이터널블루 공격은 각각 다른 접근 방식을 사용하지만, 모두 SMB 프로토콜의 취약점을 악용하는 데 공통점이 있다. 하지만 교육적인 측면에서 본다면, 내가 수행한 이터널블루 공격은 보안 실습 환경에서 더 직관적이고 강력한 교육적 도구가 될 수 있다. 그 이유는 이터널블루 공격을 통해 학생들이 직접 시스템을 장악하는 과정을 경험할 수 있기 때문이다. 시스템 제어권을 획득하고, 네트워크 상에서 추가적인 침투가 가능해지는 과정을 눈으로 확인할 수 있기 때문에, 이러한 실습은 학생들이 보안 취약점의 심각성을 체감하는 데 매우 효과적이다.

이에 비해 SMB 릴레이 공격은 인증 정보를 탈취하고 시스템에 접근하는 과정을 다루기 때문에, 네트워크 인증 시스템의 중요성을 강조하는 데는 효과적일 수 있지만, 실습 환경에서 공격 결과를 직접적으로 체감하는 데에는 상대적으로 덜 직관적일 수 있다. 이터널블루는 실습자가 취약점 공격의 결과를 직접적으로 확인하고, 공격 이후 시스템이 어떻게 손상되는지를 즉각적으로 알 수 있기 때문에 보안 교육 측면에서 훨씬 더 교육적이며, 실습 환경에서의 체험 효과가 크다. 이를 통해 이터널블루 기반의 실습은 보안 초보자들에게도 보다 명확한 보안 취약점에 대한 인식을 심어줄 수 있다.

따라서, SMB 릴레이 공격이 네트워크 인증의 취약점을 탐구하는 데 유용할 수 있는 반면, 내가 수행한 이터널블루 기반의 모의 침투 실습은

시스템 제어권 획득과 보안 취약점의 실질적인 영향력을 더 직관적으로 보여줌으로써 보안 교육에 더 효과적이다.

## 2.5 이터널블루(EternalBlue) 악용 사례

### 2.5.1 이터널블루와 관련된 주요사건

이터널블루(EternalBlue)는 다양한 사이버 공격에서 악용되었으며, 그 중 대표적인 사례로는 워너크라이(WannaCry) 랜섬웨어와 낫페트야(NotPetya) 공격이 있다.

#### 2.5.1.1 워너크라이(WannaCry) 랜섬웨어 공격

워너크라이(WannaCry) 랜섬웨어 공격은 2017년 5월에 발생한 대규모 사이버 공격으로, 150,444개국 이상에서 230,000대 이상의 컴퓨터에 영향을 미친 후 전 세계의 주목을 받았다. 병원 및 통신, 가스, 전기 및 기타 서비스 제공 업체와 같은 유명 조직이이 공격의 첫 번째 희생자였다.[5] 이터널블루를 통해 SMB 프로토콜의 취약점을 악용하였으며, 피해자들의 데이터를 암호화한 후 금전을 요구하는 방식으로 작동하였다. 이 공격은 주로 보안 패치를 적용하지 않은 시스템을 대상으로 하여, 병원, 은행, 공공 기관 등 다양한 분야에 큰 피해를 입혔다.

---

5) B. Fiore, K. Ha, L. Huynh, J. Falcon, R. Mendiola and Y. Li, "Security Analysis of Ransomware: A Deep Dive into WannaCry and Locky," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2023, pp. 285-294, doi: 10.1109/CCWC57344.2023.10099114. https://ieeexplore.ieee.org/document/10099114

#### 2.5.1.2 낫페트야(NotPetya) 공격

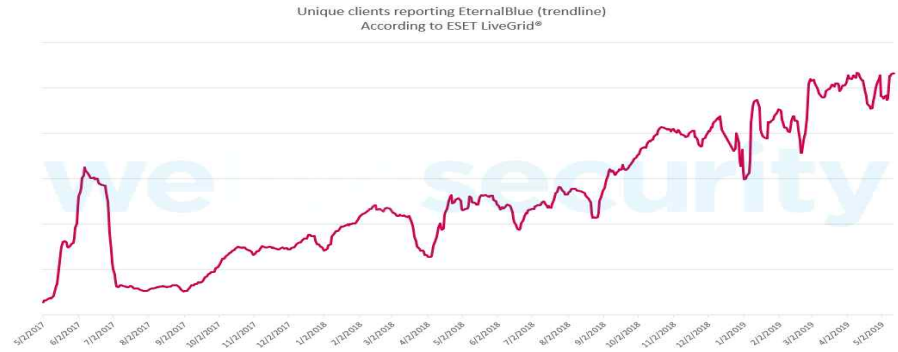
낫페트야 공격은 2017년 6월에 발생한 또 다른 대규모 사이버 공격으로, 이터널블루를 이용하여 시스템을 감염시켰다. 처음에는 우크라이나를 겨냥한 공격으로 시작되었으나, 이후 전 세계로 확산되었다. 낫페트야는 워너크라이와 유사하게 SMB 프로토콜의 취약점을 이용하였으나, 워너크라이와는 달리 데이터 복구할 수 없는 파괴적인 특성을 가지고 있었다. 이 공격으로 인해 여러 대기업과 공공 기관이 심각한 피해를 입었으며, 특히 Maersk, Merck 등 글로벌 기업들이 큰 손실을 입었다.

### 2.5.2 사건의 발생 배경과 영향

이터널블루를 활용한 사이버 공격들은 주로 패치되지 않은 취약한 시스템을 목표로 하였다. 쉐도우 브로커스에 의해 NSA의 해킹 도구가 유출된 후, 이터널블루는 사이버 범죄자들에 의해 널리 사용되었으며, 이는 전 세계적으로 큰 혼란을 야기했다. 특히, 이터널블루를 이용한 워너크라이와 낫페트야 공격은 수많은 컴퓨터 시스템을 마비시키고, 경제적으로도 막대한 손실을 초래하였다. 이터널 블루가 나타난 이후로 ESET 원격 측정에 따르면, EternalBlue와 관련된 공격 시도는 역사상 최고치에 도달하고 있으며, 다음 그림에서 볼 수 있듯이 매일 수십만 건의 인스턴스가 차단되고 있을 뿐만 아니라 악용 시도까지 이루어지고 있다.[6)]

6) https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/


[표 2-1] EternalBlue detection (trendline)




[표 2-2] Unique clients reporting EternalBlue (trendline)

### 2.5.3 사건의 결과와 교훈

이터널블루를 이용한 사이버 공격은 시스템 보안 취약점의 중요성을 강조하는 계기가 되었다. 이러한 사건들은 보안 패치의 중요성과 신속한 업데이트의 필요성을 일깨워 주었으며, 조직들은 이를 통해 보안 체계를 강화하고, 미래의 위협에 대비하기 위한 보다 엄격한 보안 정책을 수립하게 되었다.

## 2.6 이론적 배경 요약

### 2.6.1 보안 공격의 중요성과 이터널블루의 위치

사이버 보안에서 보안 공격의 중요성은 나날이 증가하고 있다. 다양한 형태의 보안 공격이 전 세계적으로 빈번하게 발생하면서, 정보 시스템에 대한 보호와 예방이 기업 및 정부 기관의 주요 과제가 되었다. 이터널블루는 이러한 보안 공격 중에서도 매우 중요한 위치를 차지하는 취약점 익스플로잇으로 조직은 시스템과 정보의 보안을 유지하기 위해 경계를 늦추지 않고 새로운 위협에 지속적으로 적응해야 한다.[7] 2017년에 발생한 워너크라이(WannaCry) 랜섬웨어와 낫페트야(NotPetya)와 같은 대규모 공격은 이터널블루를 악용하여 이루어졌으며, 이는 이 취약점이 얼마나 치명적일 수 있는지를 단적으로 보여준다. 이터널블루와 같은 고도화된 해킹 도구는 공격자에게 광범위한 공격 벡터를 제공하며, 특히 패치되지 않은 시스템을 대상으로 원격 코드 실행이 가능하다는 점에서 큰 위협이 되고 있다.

이터널블루는 네트워크 보안 취약점의 대표적인 사례로, 이러한 공격 벡터가 어떻게 실제 환경에서 악용될 수 있는지를 이해하는 것이 중요하다. 이를 통해 보안 담당자들은 보다 강력한 보안 정책을 수립하고, 취약점 관리 및 패치의 중요성을 재인식할 수 있게 된다.

### 2.6.2 이론적 배경이 실습 환경 구축에 미치는 영향

이터널블루와 같은 취약점 익스플로잇을 이해하는 것은 보안 실습 환경

---

7) A. D. Widegap and Y. Dewi Ward Hana Aznar, "Integrated Exploit Kit for Web Application," 2019 International Conference on Electrical Engineering and Computer Science (ICECOS), Bantam, Indonesia, 2019, pp. 299-302, doi: 10.1109/ICECOS47637.2019.8984449. https://ieeexplore.ieee.org/document/8984449

을 구축하는 데 중요한 영향을 미친다. 이론적 배경을 바탕으로 한 실습 환경은 실제 공격 시나리오를 재현하고, 보안 전문가들이 대응 및 예방 전략을 연습할 수 있는 중요한 훈련 도구가 된다. 이터널블루의 공격 원리와 취약점 악용 사례를 이해함으로써, 실습자는 시스템의 보안 취약점을 분석하고, 이를 악용하는 공격을 방어하는 방법을 효과적으로 학습할 수 있다.

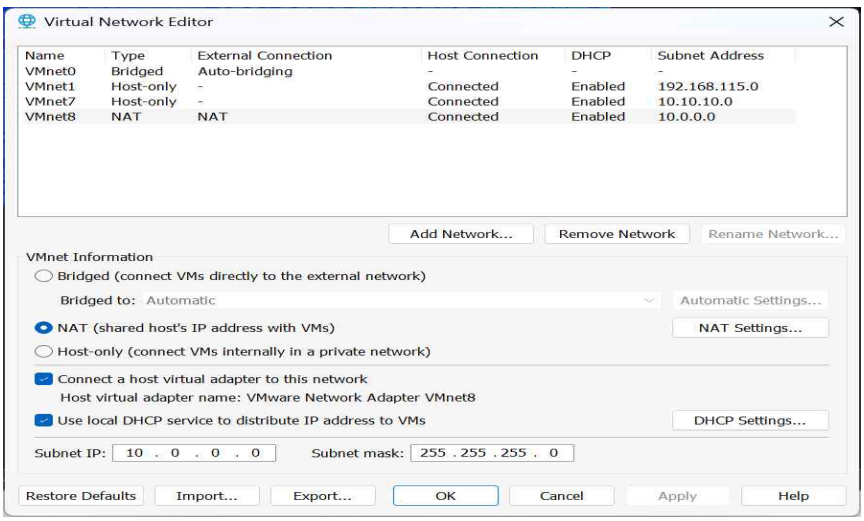
실습 환경에서는 이러한 이론적 배경을 바탕으로 실제 취약점을 재현하고 이를 통해 보안 시스템을 강화하는 데 필요한 기술을 익히게 된다. 특히 Windows Server와 같은 운영체제를 대상으로 하는 실습에서는 이터널블루와 같은 취약점이 어떻게 네트워크 내에서 악용되는지를 이해하고, 이를 방어하기 위한 보안 정책 수립 및 패치 적용의 중요성을 체득하게 된다. 이론적 지식과 실습 경험을 결합함으로써 보안 실무자는 실제 환경에서 더욱 신속하고 효과적으로 대응할 수 있는 능력을 배양할 수 있다.

# 제 3 장 환경구축 및 실습

## 3.1 환경구축

### 3.1.1 VMware Workstation Pro 설치

이제는 이전의 이론을 바탕으로 실제 환경을 구축하는 단계로 넘어가 보자. 주요하게 설치해야 할 프로그램은 VMware Pro, Kali Linux, 그리고 Windows Server 2012 R2이다. VMware는 가상 환경에서 다양한 운영체제를 설치하고 관리할 수 있는 소프트웨어로, 물리적 메모리 절약뿐만 아니라 공격 실험을 위한 랩을 손쉽게 구성할 수 있다는 장점이 있다. 이로 인해 호스트 PC에 직접적으로 영향을 미칠 수 있는 프로그램이나 스크립트를 가상 환경에서 안전하게 테스트할 수 있어 사이버 보안 실습에 매우 적합하다.

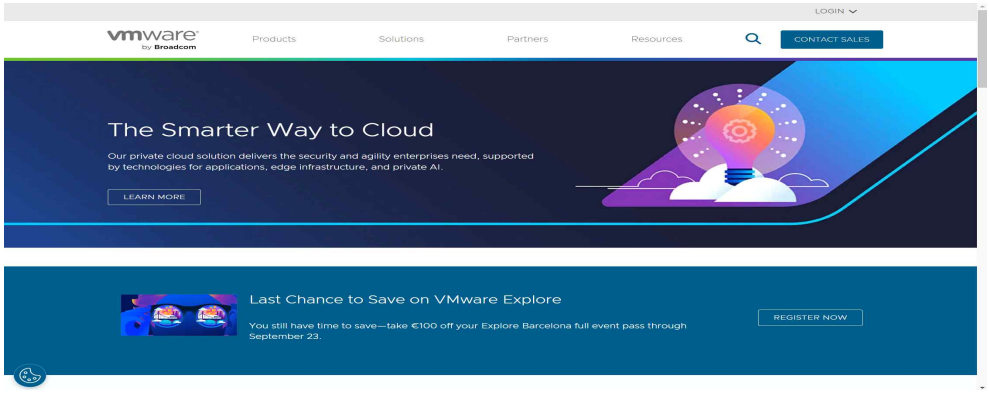



[그림 3-1] Virtual Network Editor

처음 사용 시 VMware의 다양한 기능은 다소 복잡하게 느껴질 수 있지만, 운영체제를 몇 번 설치하고 삭제하는 과정을 거치면 쉽게 익숙해질 수 있다. VMware는 무료 버전과 유료 Pro 버전으로 나뉘는데, 본 실험

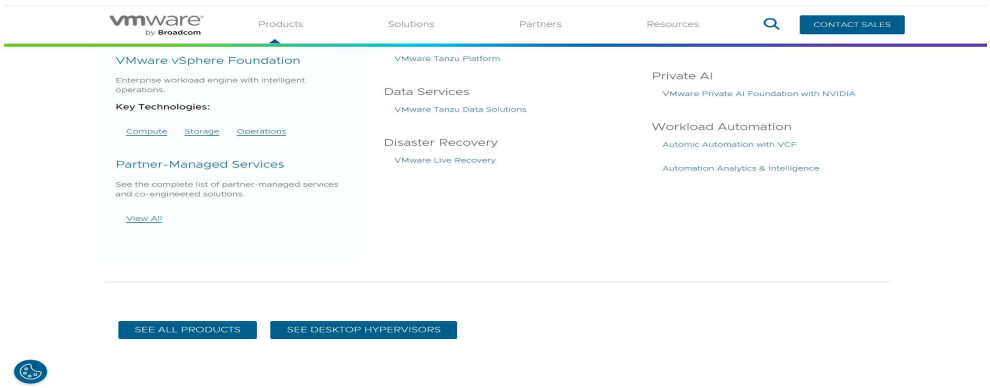
에서는 Pro 버전 사용을 권장한다. 그 이유는 Pro 버전에서만 제공되는 VMware Network Editor를 통해 네트워크 설정을 커스터마이징할 수 있기 때문이다. 네트워크 설정은 Kali Linux와 Windows Server를 동일한 네트워크에 두어 상호 통신 및 공격이 가능하도록 해주는 필수적인 과정이다. 필자는 처음 Kali Linux와 Windows Server를 같은 VMware 환경에 설치하였음에도 불구하고, 통신이 되지 않아 많은 시행착오를 겪었다. 특히, 기본적인 ping 명령조차 정상적으로 이루어지지 않아 문제 해결에 상당한 시간을 소요하였다. 이를 해결하기 위해서는 VMware의 네트워크 설정, 특히 NAT, Host-only, Custom 옵션 등을 적절히 구성해야 한다. Pro 버전을 사용하지 않았을 때는 Network Editor 기능이 제공되지 않기 때문에, 필자는 해당 기능을 찾느라 불필요한 시간과 노력을 소비하게 되었다. 따라서 이 논문을 읽는 학습자들은 반드시 VMware Pro 버전을 설치하여 실습할 것을 권장한다. 많은 이들이 Pro 버전을 사용하기 위해 추가적인 비용이 발생할 것으로 생각할 수 있지만, 현재 VMware는 Pro 버전을 무료로 제공하는 프로모션을 시행하고 있다. 다음 섹션에서는 이 Pro 버전을 무료로 설치하는 방법과 네트워크 설정 절차를 보다 자세히 설명하고자 한다.

이렇게 구성한 내용은 이론과 실습을 결합하여 학습자가 실제 환경에서 체계적으로 사이버 보안 실습을 수행할 수 있도록 돕는 것을 목표로 한다.



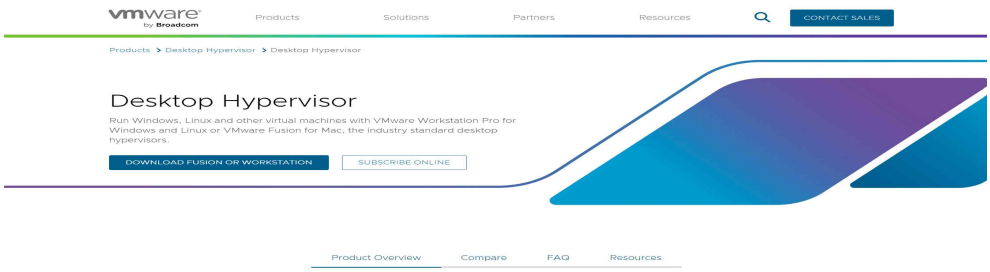

[그림 3-2] Vmware 홈페이지

첫째로 그림3-2처럼 VMware 홈페이지에 접속한다.



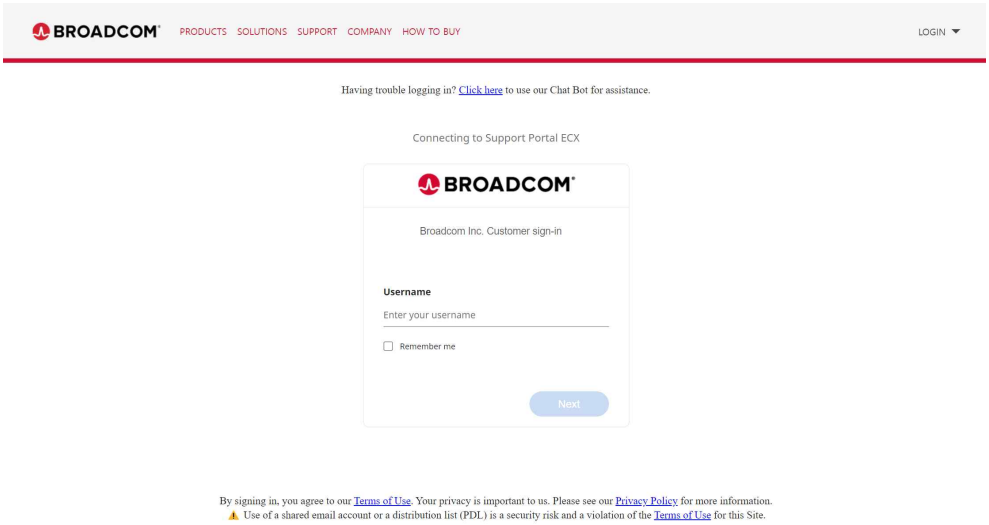

[그림 3-3] Products 메뉴 바

두 번째로 상단의 Products 바를 클릭 후 아래로 스크롤 하여 SEE DESKTOP HYPERVISORS 박스를 클릭한다.



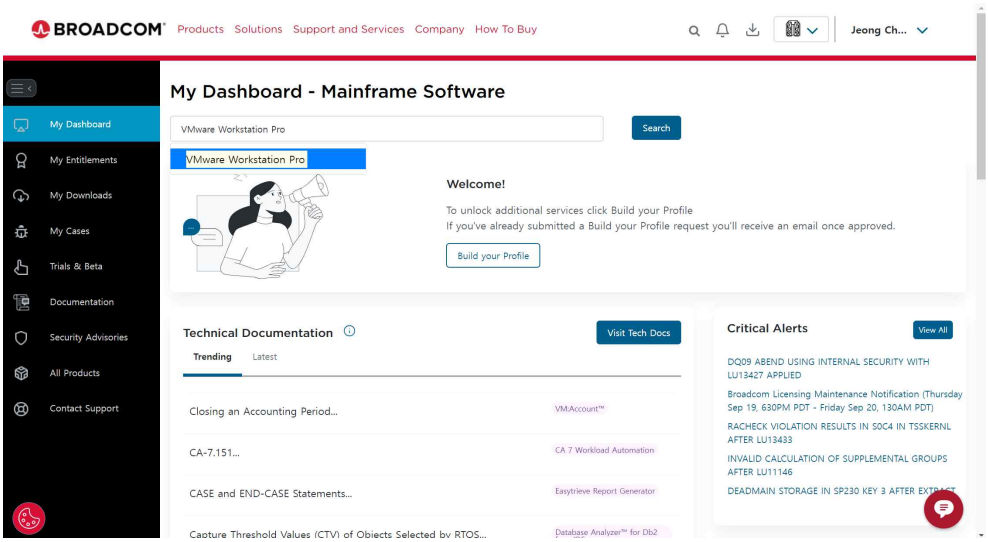

[그림 3-4] Desktop Hyper visor 화면

그 이후 DOWNLOAD FUSION OR WORKSTATION 바를 클릭한다.



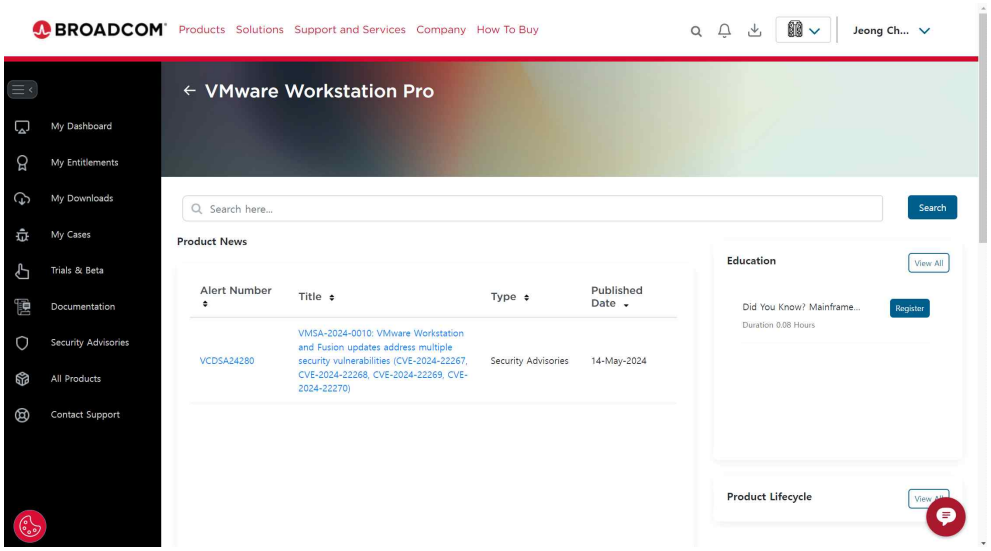

[그림 3-5] BROADCOM 로그인 페이지

BROADCOM 로그인 페이지가 나타나게 된다. 우리는 여기서 회원가입을 해야 한다. 오른쪽 위의 LOGIN 버튼을 클릭하여 회원가입을 진행한 후 Username과 비밀번호기입을 한다.



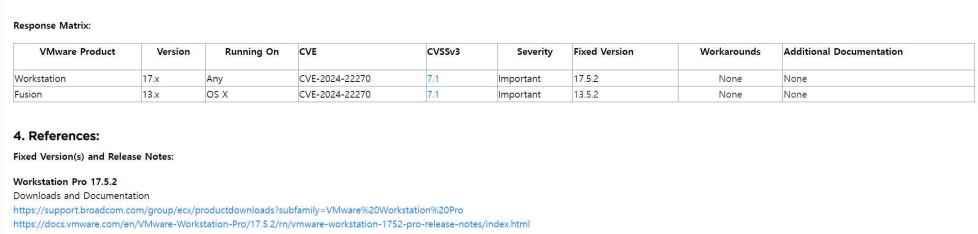

[그림 3-6] My Dashborad

로그인에 성공했다면 왼쪽 바의 MyDashboard 바를 선택한 후 중앙 검색 창에 VMware Workstaion Pro를 입력하고 Search 버튼을 클릭한다.




[그림 3-7] Product News

그렇게 찾아진 VMware Pro 타이틀 링크를 클릭한다.



**Response Matrix:**

| VMware Product | Version | Running On | CVE | CVSSv3 | Severity | Fixed Version | Workarounds | Additional Documentation |
|---|---|---|---|---|---|---|---|---|
| Workstation | 17.x | Any | CVE-2024-22270 | 7.1 | Important | 17.5.2 | None | None |
| Fusion | 13.x | OS X | CVE-2024-22270 | 7.1 | Important | 13.5.2 | None | None |

**4. References:**

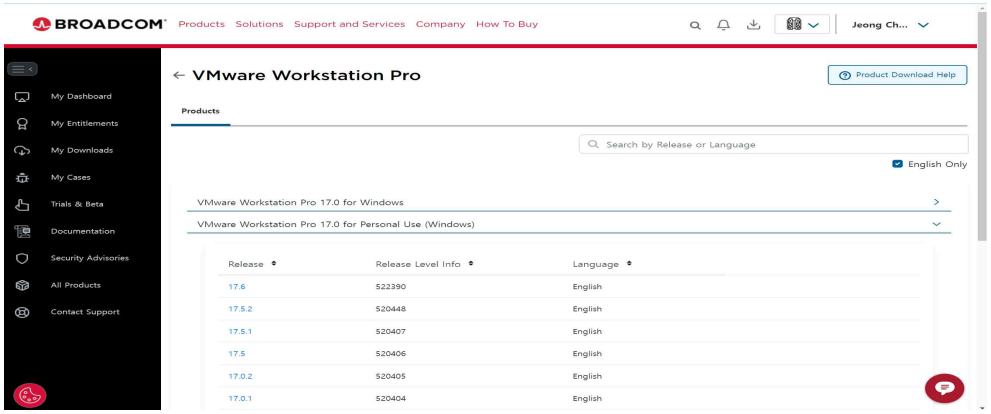
**Fixed Version(s) and Release Notes:**

**Workstation Pro 17.5.2**
Downloads and Documentation
https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware%20Workstation%20Pro
https://docs.vmware.com/en/VMware-Workstation-Pro/17.5.2/rn/vmware-workstation-1752-pro-release-notes/index.html

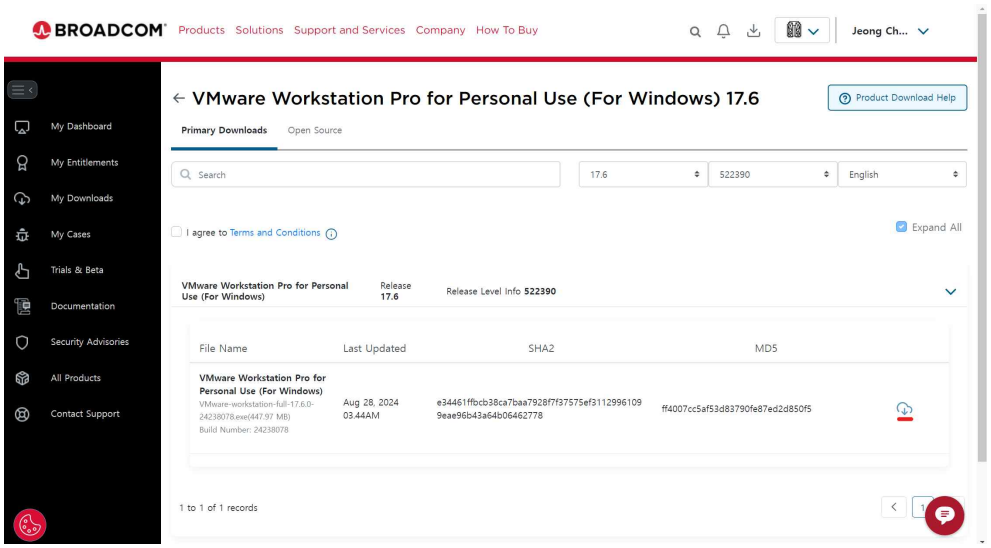
[그림 3-8] Downloads

링크에 접속하게 된 후 아래로 스크롤을 하면 4. Refernces 항목에서 다운로드 링크를 찾을 수 있다. 마지막이 Pro로 끝나는 링크를 클릭한다.

링크에 접속하게 되면 각 운영체제에 맞는 다운로드 파일을 선택할 수 있는데 무료로 설치하기 위해서는 Personal Use라고 기입되어 있는 Windows와 Linux 둘 중 본인의 호스트 PC의 운영체제에 맞는 릴리스 파일을 다운로드 하기를 바란다.




[그림 3-9] Downloads 2

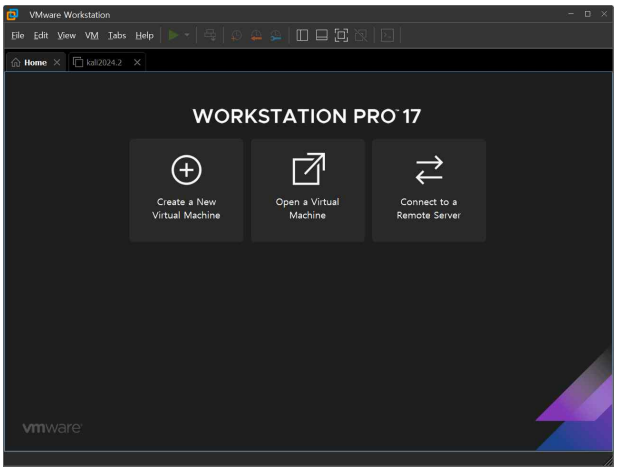



[그림 3-10] Downloads 3

원하는 릴리스 버전을 클릭 하면 마지막 다운로드를 할 수 있는 창이 나오게 되는데 바로 다운로드 할 수 없다. 먼저 I agree to Terms and Conditions라는 항목을 체크를 하고 중앙 오른쪽 구름 모양의 아이콘을 클릭 하면 Trade Compliance Verification 페이지가 나오게 되는데 *표시로 된 항목들을 모두 채운 후 Submit을 한 뒤 다시 그림 3-10으로 돌아와 구름 모양의 아이콘을 클릭하면 최종적으로 실행파일을 내려받을 수 있게 된다.


[그림 3-11] Personal Use

최종적으로 내려받은 VMware 설치 파일을 다른 설치 프로그램들과 같은 방식으로 설치를 한 후 실행을 시키면 그림 3-11과 같은 창이 나타나며 key 번호를 요구한다. 하지만 이때 키 번호를 입력하는 것이 아닌 Use VMware Workstation 17 for Personal Use 란을 선택한다.




[그림 3-12] VMware Workstation

그렇게 되면 최종적으로 VMware Workstation을 실행할 수 있게 된다.

### 3.1.2 kali Linux 설치

Kali Linux는 정보 보안 및 침투 테스트를 위해 개발된 전문 운영체제로, 보안 연구와 실습에서 널리 사용되고 있다.[8] 보안 취약점 분석, 네트워크 침투 테스트, 디지털 포렌식 등 다양한 보안 관련 작업을 수행할 수 있는 도구들이 사전 설치되어 있으며, 이러한 특성 덕분에 보안 전문가들과 해커들이 주로 사용하는 환경 중 하나이다. Kali Linux는 오픈소스 기반으로 개발되었고, Debian 기반의 안정적인 시스템을 바탕으로 다양한 해킹 도구와 보안 테스트 도구를 통합하고 있어 사용자들이 별도의 설치나 설정 없이도 즉시 다양한 보안 실습을 진행할 수 있다.

이 운영체제는 윈도우 서버와 같은 시스템에 대한 침투 테스트를 진행할 때 중요한 역할을 한다. 특히, 본 논문에서 다루고 있는 이터널블루(EternalBlue) 공격과 같은 취약점 악용 실습을 진행하는 데 적합한 환경을 제공한다. 이를 통해 공격 벡터를 분석하고, 실습으로 보안 취약점이 시스템에 미치는 영향을 확인하며, 이에 대한 방어 전략을 연구할 수 있다.

Kali Linux를 설치하기 위해서는 먼저 Kali Linux 공식 웹사이트에서 최신 버전의 ISO 이미지를 다운로드해야 한다. 내려받은 이미지를 이용해 VMware에서 가상 머신을 생성하고, 가상 환경에서 설치를 진행한다. 설치 과정은 비교적 간단하며, 인터넷 검색을 통해서도 충분히 할 수 있는 영역이기에 그림을 포함한 자세한 설치 과정은 생략한다. 설치가 완료되면 Kali Linux 내에 포함된 다양한 보안 도구를 활용하여 침투 테스트 및 기타 보안 실습을 바로 시작할 수 있다. 이를 통해 연구자는 실습 환경을 완성하고, 윈도우 서버의 취약점 분석과 같은 실무적인 테스트를 진행할 수 있다.

### 3.1.3 Windows server 2012 R2 설치

Windows Server 2012 R2는 기업 환경에서 널리 사용되는 서버 운영체제로, 다양한 네트워크 관리, 데이터 저장, 애플리케이션 실행 등의 기능을 제공한다. 보안 측면에서는 서버의 역할과 기능이 중요한 만큼, 이를 침투 테스트 및 보안 분석 대상으로 사용하는 것은 매우 의미 있는 실습이다. 특히, 이터널블루(EternalBlue)와 같은 SMB 프로토콜 취약점을 악용한 공격의 사례에서 주로 타겟이 되는 시스템이기도 하다.

---

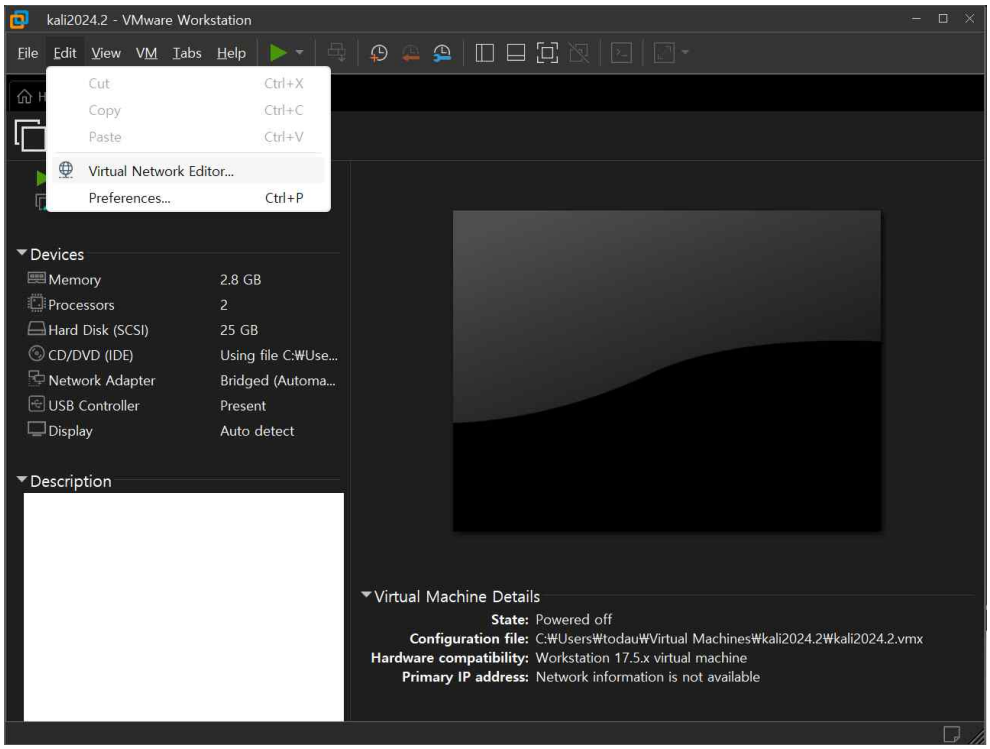
8) 김승우. "자율주행차량과 AI 드론봇에 대한 해킹 공격 및 취약점 보안 연구." 국내박사학위논문 호서대학교 벤처대학원, 2020. 충청남도 115p.

Windows Server 2012 R2를 설치하기 위해서는 먼저 Microsoft의 공식 웹사이트 또는 정식 라이선스를 통해 설치 파일을 준비해야 한다. 설치 파일을 준비한 후, 이를 VMware와 같은 가상화 환경에서 실행할 수 있도록 설정한다. VMware에서 새로운 가상 머신을 생성한 뒤, 서버 운영체제를 설치하는 과정은 일반적인 윈도우 설치 절차와 유사하다. 설치가 완료되면 서버 역할을 설정하고, 네트워크 구성 및 기본적인 보안 설정을 통해 실습 환경을 구성할 수 있다.

Windows Server 2012 R2는 다양한 네트워크 서비스와 서버 관리 기능을 제공하기 때문에, 이를 통해 네트워크 구조와 보안 취약점에 대한 실습을 더욱 구체적으로 진행할 수 있다. 또한, 윈도우 서버는 실제 기업 환경에서도 자주 사용되기 때문에 보안 연구에서 필수적인 플랫폼으로 간주한다. 이와 같은 이유로 Windows Server 2012 R2는 이터널블루 공격의 실습 환경에서 매우 중요한 역할을 하며, 이를 통해 실제 취약점을 탐구하고 방어 전략을 수립하는 과정이 가능해진다. 동일하게 Windows Server 2012 R2를 Vmware에 작성하는 방법 또한 인터넷 검색을 통해 설치를 완료한다.

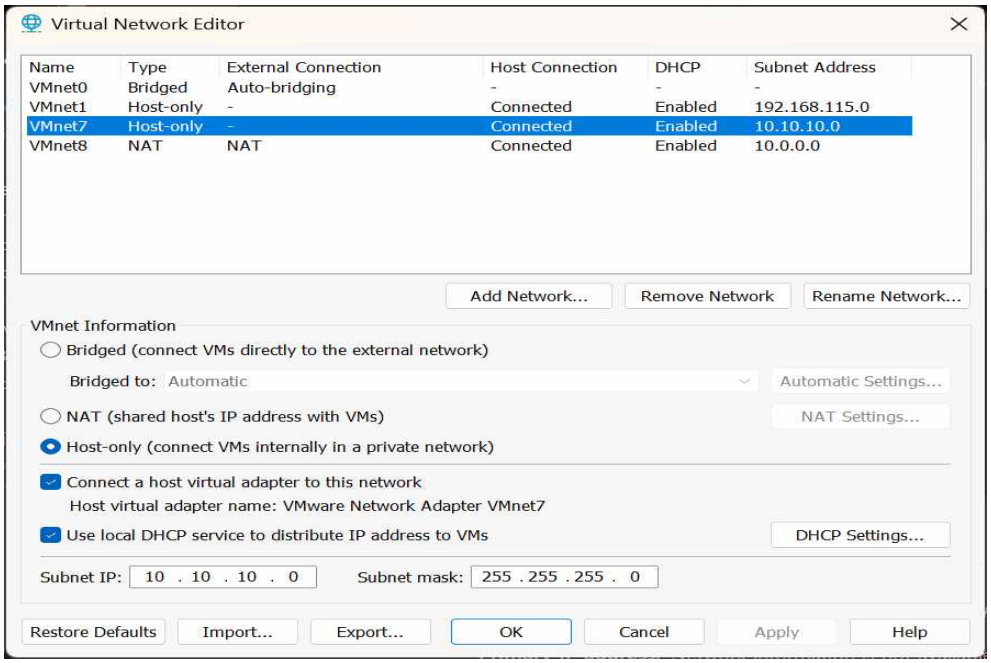
### 3.1.4 모의 침투용 Kali Linux 환경구축

칼리 리눅스가 VMware에 정상적으로 설치가 되었다면 사용자가 직접 기본적인 모의 침투용 환경구축을 해 주어야 한다. 먼저는 VMware editor를 통해 네트워크 설정을 해야 한다.



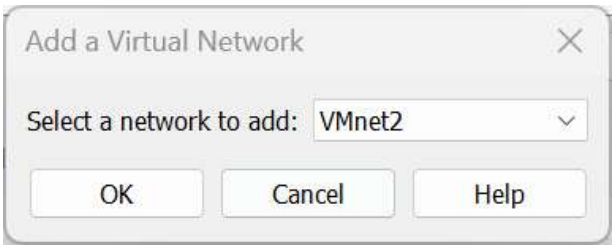

[그림 3-13] virtual Network Editor 1

VMware 초기 화면에서 Edit 메뉴에서 Virtual Network Editor를 클릭한다.



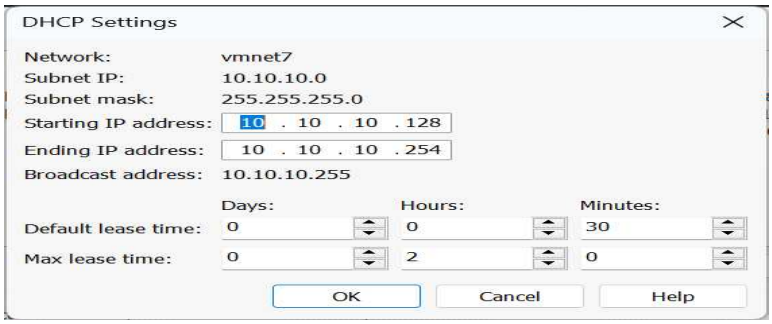

[그림 3-14] Virtual Network Editor

Virtual Network Editor에서는 IP,Subnet mask,Type을 설정할 수 있다. 먼저 중앙에 Add Network... 버튼을 클릭하여 새로운 네트워크를 추가 할 것이다.




[그림 3-15] Add a Virtual Network

Select a network to add를 통해 새로운 VMnet을 추가할 수 있다. 본 연구에서는 VMnet7을 선택하였다.




[그림 3-16] DHCP Settings

그 후 VMnet7을 선택 후 DHCP Settings 버튼을 누르면 이러한 창이 화면에 출력된다. 여기서는 시작 IP 주소와 끝나는 IP 주소를 설정할 수 있다. 대역대는 10.10.10을 선택했고 시작 주소는 128, 끝 주소는 254로 설정한다. 그리고 그림 [3-14]처럼 Subnet IP를 10.10.10.0 Subnet mask는 255.255.255.0 으로 설정 한다. Windows server와 동일한 네트워크에서 실험을 진행해야 하기 때문이다. 설정을 다 마친 후에는 OK 버튼을 눌러 설정을 적용한다.

### 3.1.5 모의 침투용 Windows server 2012 R2 환경구축

피해자 PC인 Windows server 2012 R2 또한 VMware에 설치를 완료했다면 여러 설정을 해 주어야 모의 침투가 가능하다.
모의 침투 테스트를 위한 Windows Server 2012 R2 환경 설정은 Kali Linux와 상호작용할 수 있는 네트워크 구성을 통해 진행된다. 이를 위해 먼저 Windows Server 2012 R2 Essentials를 설치하고, 기본적인 네트워크 설정 및 보안 규칙을 구성하는 단계가 필요하다.
우선, Microsoft의 공식 웹사이트에서 Windows Server 2012 R2 Essentials ISO 파일을 다운로드한다. 이후, VMware에 해당 ISO 파일을 사용하여 Windows Server 2012 R2를 설치한다. 설치가 완료되면, 정품 인증을 위해 제공된 인증 키를 입력하여 활성화한다. 인증키는 다운로드 페이지 하단에 있다. 그런 다음, 자동 업데이트로 인해 서버가 예기치 않게 재부팅되는 것을 방지하기 위해 윈도우 업데이트 설정을 수동으로 변경한다.
네트워크 환경을 설정하는 단계로는 먼저 VMware의 네트워크 어댑터를 NAT 방식에서 사용자 지정 VMnet8로 변경하고, IP 주소와 DNS 설정을 수동으로 지정한다. 기본적으로 IPv4 속성에서 IP 주소는 10.0.0.27, 서브넷 마스크는 255.255.255.0, 게이트웨이는 10.0.0.2로 설정하며, DNS 서버는 8.8.8.8과 8.8.4.4로 설정하여 인터넷 연결이 가능하도록

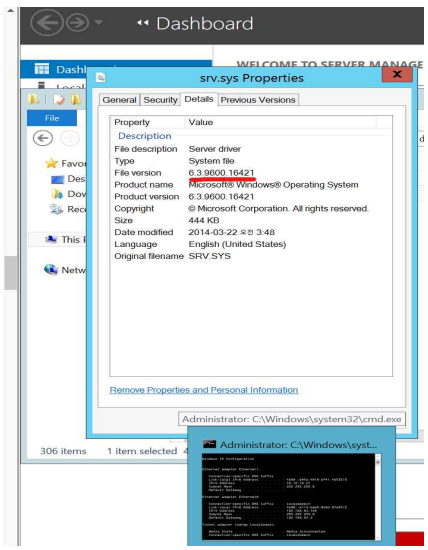
한다.
이후, [그림3-14]와 동일하게 두 번째 네트워크 어댑터를 추가하여 이를 Custom VMnet7으로 설정하고, 해당 어댑터의 IPv4 속성 역시 수동으로 지정한다. 이때 IP 주소는 10.10.10.27, 서브넷 마스크는 255.255.255.0, 게이트웨이는 10.10.10.2로 설정하며, DNS 서버는 앞서와 동일하게 8.8.8.8과 8.8.4.4로 설정한다. 이는 Kali Linux와 동일한 네트워크 대역 내에서의 통신을 가능하게 하여 모의 침투 실습 환경을 구축하는 데 필수적이다.
다음으로, Kali Linux의 네트워크 설정을 vi 편집기를 통해 변경하여 eth0 인터페이스에 10.10.10.128로 설정하고 Windows Server와 동일한 네트워크 대역을 사용하도록 한다. 이에 따라 두 시스템 간의 상호 통신이 가능해진다.
Windows Server에서는 방화벽 설정을 수정하여 인바운드 규칙에서 파일 및 프린터 공유와 관련된 ICMPv4 규칙을 활성화하고, 원격 데스크톱을 위한 TCP 규칙도 활성화한다. 이를 통해 외부 장치에서 Windows Server에 대한 접근과 네트워크 테스트가 가능해진다. 설정이 완료되면, Kali Linux에서 Windows Server의 IP 주소로 핑 테스트를 실행하여 네트워크 연결이 정상적으로 이루어졌는지 확인한다. 여기서 eth1 인터페이스를 통한 10.10.10.27로의 핑 테스트와 eth0 인터페이스를 통한 10.0.0.27로의 핑 테스트를 모두 수행한다. 반대로, Windows Server에서도 Kali Linux로 핑 테스트를 진행하여 두 시스템 간의 통신이 원활하게 이루어졌는지 확인한다.
그 다음 단계로는 파일 공유 설정을 통해 Kali Linux와 Windows Server 간 파일을 주고받을 수 있도록 구성하며, PowerShell을 사용하여 SMB 프로토콜이 활성화되어 있는지 확인한다. 만약 SMB 설정을 하지 않을 시 다음 그림과 같이 SMB 취약점을 스캔했을 때 취약점이 발견되지 않으니 꼭 SMB 설정을 해 주어야 한다.

```
┌──(uchan㉿chan)-[~]
└─$ sudo nmap --script smb-vuln* -p 445 10.10.10.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 16:55 KST
Nmap scan report for 10.10.10.27
Host is up (0.00071s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:76:37:77 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: No accounts left to try

Nmap done: 1 IP address (1 host up) scanned in 18.55 seconds
```

[그림 3-17] SMB 취약점 발견되지 않는 경우

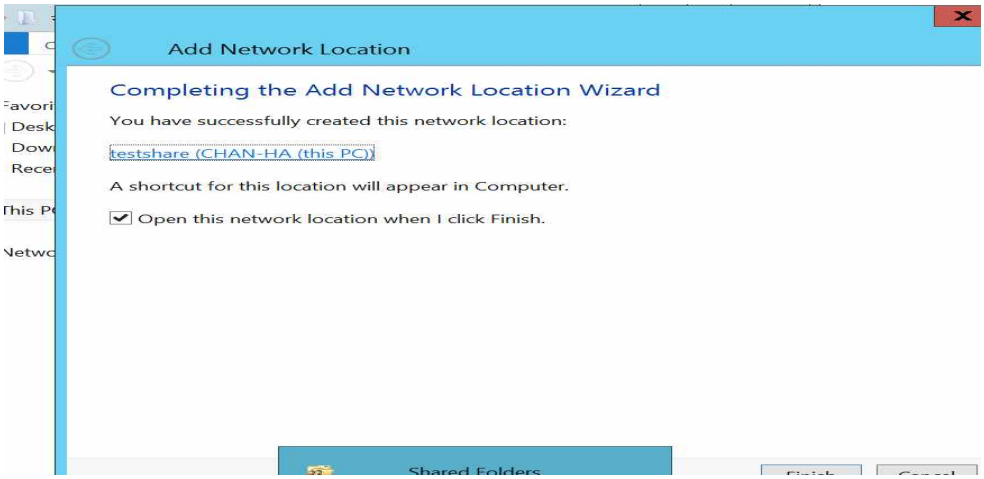
처음에는 Windows server 2012 R2 운영체제 자체가 SMB 취약점이 존재하지 않는 버전인가 라고 생각이 들어 다른 운영체제를 사용할까, 고민하였지만 아래 [그림 3-18] 처럼 공식 문서를 대조 해 보니 버전이 원래의 설치되어 있어야 하는 버전보다 낮아서 존재한다는 것을 확인할 수 있었다.

| | |
|---|---|
| Windows XP | 5.1.2600.7208 |
| Windows Server 2003 SP2 | 5.2.3790.6021 |
| Windows Vista<br>Windows Server 2008 SP2 | GDR:6.0.6002.19743, LDR:6.0.6002.24067 |
| Windows 7<br>Windows Server 2008 R2 | 6.1.7601.23689 |
| Windows 8<br>Windows Server 2012 | 6.2.9200.22099 |
| Windows 8.1<br>Windows Server 2012 R2 | 6.3.9600.18604 |
| Windows 10 TH1 v1507 | 10.0.10240.17319 |
| Windows 10 TH2 v1511 | 10.0.10586.839 |
| Windows 10 RS1 v1607<br>Windows Server 2016 | 10.0.14393.953 |




[그림 3-18] MS17-010 설치 여부 확인

그렇기에 SMB 설정을 완료한다. 자세한 프로세스는 SMB 설정의 문서[9]를 참고하는 것을 추천한다.




[그림 3-19] 공유 폴더 생성

그 이후 마지막으로 명령어를 통해 SMB1 및 SMB2 프로토콜이 활성화 상태인지 검사한 후, SMB 관련 포트인 445번 포트를 열고 외부 공격이 가능하도록 설정한다.

## 3.2 모의 침투 실습

칼리 리눅스(Kali linux)와 Windows sever 2012 R2의 환경을 다 마친 후 실제로 칼리 리눅스를 통해 모의 침투 실습을 진행한다.

먼저는 아래의 그림과 같이 nmap --script vuln 10.10.10.27 명령어를 통해 공격하려는 대상의 OS에 우리가 찾는 ms17-010 취약점이 있는지 스캔을 시행한다. 여기서 nmap 이란

9) https://continuetochallenge.tistory.com/17

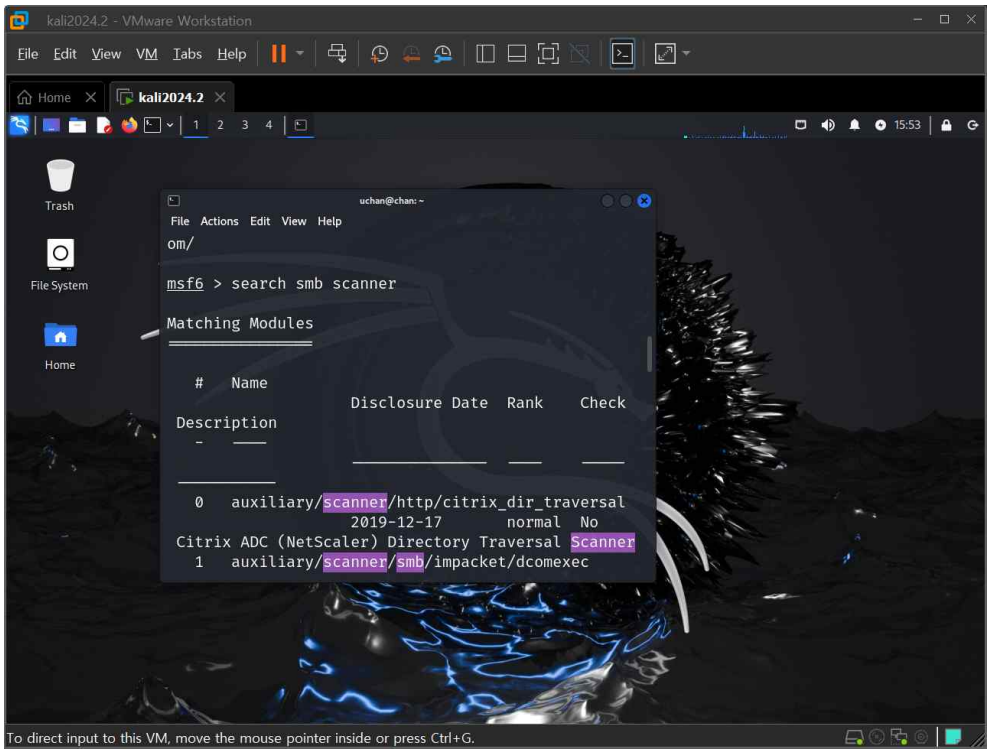
```
MAC Address: 00:0C:29:76:37:77 (VMware)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-01
0)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft
SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidan
ce-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 128.98 seconds
```

[그림 3-20] ms17-010 취약점 존재 여부 확인.

그림에서 보이듯이 smb-vuln-ms17-010 취약점에 대한 정보가 나오며 취약점이 존재한다는 사실을 확인할 수 있다.
그 이후 칼리 리눅스의 도구인 msfconsole을 사용할 것이다.

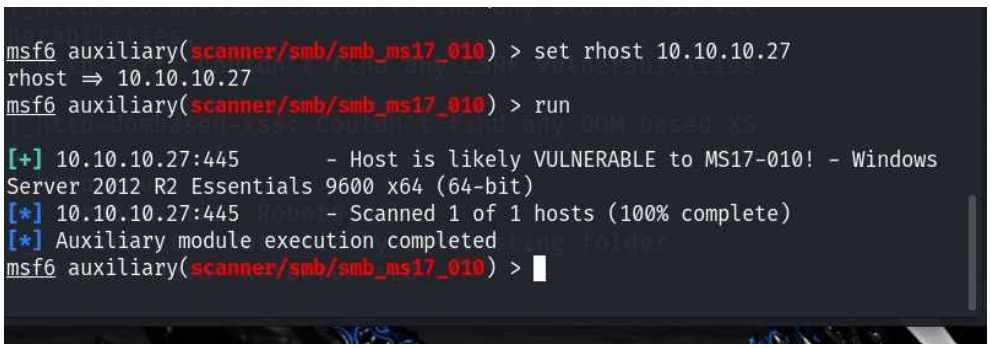

[그림 3-21]msfconsole

사용법은 간단하게 칼리 리눅스 터미널을 열고 msfconsole을 입력 해 주면 된다.



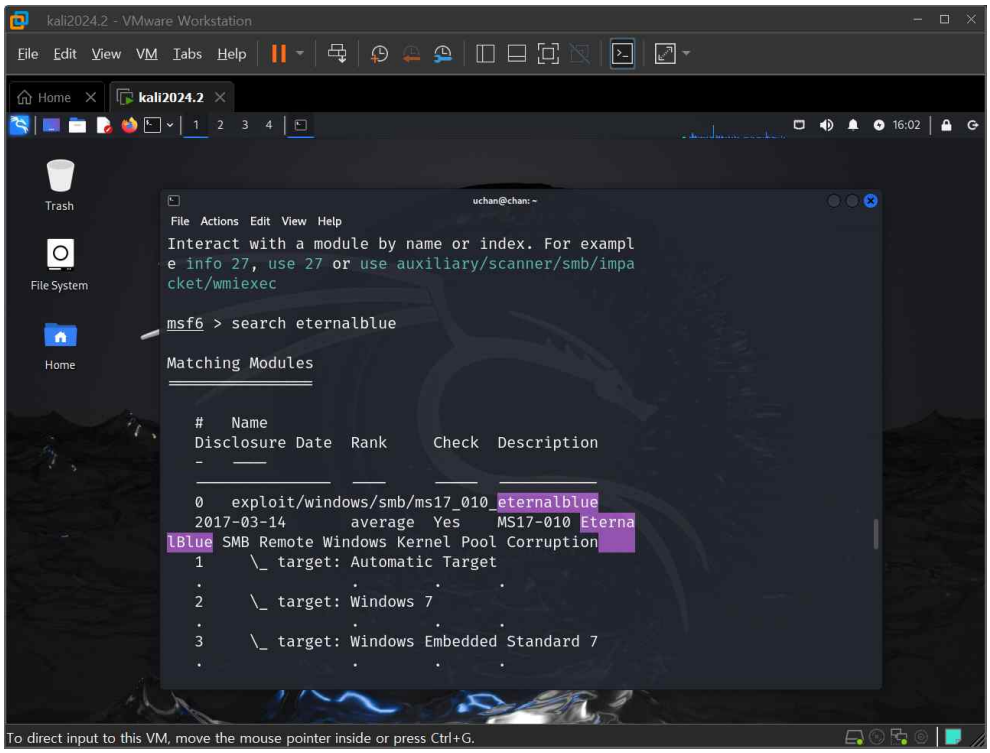

[그림 3-22] smb scanner

그리고 search smb scnner 명령어를 통해 smb 스캐너를 찾은 후 use auxiliary/scanner/smb/smb_ms17_010 을 명령어로 다시 입력하여 smb취약점을 찾는 스캐너를 사용한다.



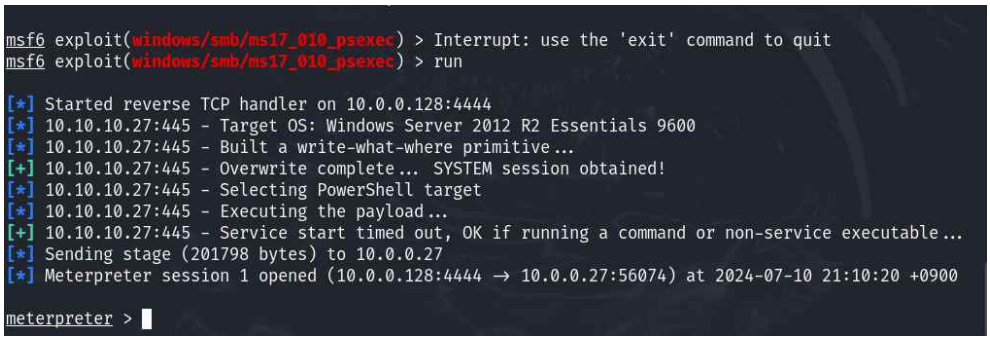

[그림 3-23] scanner 사용

대상인 Windows server 2012 R2의 IP 인 10.10.10.27을 set rhost 10.10.10.27로 옵션을 설정하고 run을 통해 실행했을 경우 Host is likely VULNERABLE to MS17-010! 문구와 함께 대상의 운영체제까지 확인 할 수 있다.




[그림 3-24] EternalBlue

이제 최종적으로 Eternalblue 공격을 시행할 수 있다. 아까와 같이 search eternalblue 명령어를 통해 사용할 버전을 골라야 하는데 이 중에서 target: Windows server 2012 가 적절할 것 같지만 이 버전을 사용하면 실패한다. 그 이유는 추후의 연구가 더 필요하다. 본 연구에서는 exploit/windows/smb/ms17_010_psexec을 사용한다. use 명령어와 함께 use exploit/windows/smb/ms17_010_psexec를 입력해 공격을 준비한다. 그리고 동일하게 옵션을 설정해 주어야 한다. set rhost 10.10.10.27, set payload windows/x64/meterpreter/revers_tcp 대상 ip와 리버스 커넥션을 위한 페이로드를 설정한 후 실행(run) 명령어를 시행한다.




[그림 3-25] meterpreter 획득

정상적으로 공격이 실행되었다면 meterpreter 세션을 획득할 수 있다. Meterpreter 세션이 확보된 이후, 공격자는 내부 시스템을 더 깊이 파고들어 권한을 상승시키거나, 네트워크의 다른 기기들로 공격을 확장할 수 있는 잠재력을 가지게 된다. 이는 단순한 침투 이상의 위협을 의미하며, 데이터 유출, 시스템 기능 마비, 심지어 전체 네트워크의 장악으로 이어질 수 있는 매우 심각한 상황을 초래할 수 있다. 이 후로는 SMB취약점을 활용한 또 다른 방식의 모의침투 방식을 제시하며 필자의 연구와 비교하며 어떠한점에서 필자의 모의침투 방식이 더 효과적이며 교육적인지에 대해 심도있게 알아보고자 한다.

# 제 4 장 결론

## 4.1 연구 결과

이번 연구에서 수행된 이터널블루 기반의 모의 침투 실습은 기존의 다른 모의 침투 방법론들과 비교해 여러 면에서 구체적으로 우수한 교육적, 기술적 이점을 제공하였다. 이터널블루 공격은 SMB 취약점을 이용하여 시스템 전체를 제어할 수 있는 매우 강력한 익스플로잇으로, VulnHub의 기본적인 취약점 실습이나 SMB 릴레이 공격에 비해 훨씬 직관적이고, 학습 효과가 뛰어나다는 점에서 우위를 점하고 있다.

첫째, VulnHub 기반의 실습은 기본적으로 다양한 취약점을 학습하는 데 유용하지만, 그 복잡도와 시스템 제어에 대한 심도는 이터널블루 공격과 비교했을 때 상대적으로 낮다. VulnHub 실습에서는 시스템 내 특정 서비스나 애플리케이션의 취약점을 중심으로 이루어지며, 이터널블루처럼 전체 시스템의 권한을 획득하는 과정보다는 개별적인 취약점에 초점을 맞춘다. 이에 비해 본 연구에서는 Windows Server 2012 R2와 같은 실제 환경에서 Kali Linux를 사용하여 직접 공격을 수행하는 과정에서, 학습자가 SMB 취약점을 실제로 체감하고 이를 통해 공격자가 시스템 전반을 장악할 수 있다는 점을 더 깊이 있게 학습할 수 있었다. 이는 실제 상황에서 시스템 취약점이 어떻게 악용될 수 있는지에 대한 이해를 더욱 효과적으로 전달한다.

둘째, SMB 릴레이 공격은 SMB 프로토콜의 인증 절차를 공격하는 기법으로, 이터널블루에 비해 시스템 장악의 범위가 제한적이다. SMB 릴레이는 주로 인증 정보를 탈취하는 데 중점을 두며, 공격 범위는 인증 과정에 머무르는 경우가 많다. 반면 이터널블루는 SMB 취약점을 통해 시스템의 모든 권한을 획득하는 데 목표를 두며, 이를 통해 학습자는 단순한 인증 정보 탈취 이상의 시스템 제어 경험을 할 수 있다. 이는 실제

보안 침투 상황에서 공격자가 시스템 전체를 악용하는 과정을 더욱 잘 이해할 수 있도록 도와주며, 모의 침투 실습에서 시스템의 보안 취약점이 어떤 식으로 악용되는지 구체적으로 학습할 수 있다.

셋째, Gupta et al.의 Eternal Blue Vulnerability 연구는 이터널블루가 발생한 역사적 배경과 이를 활용한 공격의 심각성을 기술하고 있으나, 본 연구는 단순한 이론적 설명을 넘어 실제로 시스템 환경을 구축하고 이를 기반으로 침투 공격을 실습한다는 점에서 더욱 교육적인 효과를 발휘한다. 실제 환경에서의 실습은 학습자에게 추상적인 개념이 아닌, 구체적인 보안 기술을 체득할 수 있는 기회를 제공하며, 이론적 지식을 바탕으로 실제 시스템에서의 취약점 악용이 어떻게 이루어지는지 이해할 수 있게 한다.

따라서 본 연구의 방법론은 이론적 설명에 머물지 않고, 실제로 학습자가 실습을 통해 시스템 제어권을 획득하는 과정까지 직접 경험하게 한다는 점에서 교육적 효과가 뛰어나다. 또한, 이를 통해 학습자는 단순한 취약점 분석을 넘어서, 시스템 전반을 보호하고 대응하는 데 필요한 실질적인 기술을 습득할 수 있다. 이러한 점에서 본 연구는 실제 보안 침투 테스트 교육에 있어 더 나은 방법론을 제시하고 있으며, VulnHub, SMB 릴레이, Gupta 등의 관련연구와 비교했을때 더욱 심층적이고 실질적인 학습 기회를 제공한다.

## 4.2 향후 연구 계획

향후 연구에서는 이터널블루와 같은 SMB 프로토콜 취약점에 대한 보다 심층적인 방어 기법과 대응 전략을 개발하는 데 초점을 맞출 예정이다. 이터널블루는 여전히 많은 시스템에서 위험 요소로 남아 있으며, 특히 패치가 적용되지 않은 구형 시스템에서는 여전히 악용될 가능성이 크다. 따라서 향후 연구에서는 이러한 취약점에 대한 보다 구체적인 대응 방안을 모색할 것이다.

첫째, 패치 적용의 자동화 및 취약점 관리 시스템을 개발하여, 보안 패치를 적용하지 못한 시스템에 대한 보호 방법을 강화할 계획이다. 이를 통해 자동으로 패치를 확인하고 적용하여, 공격자들이 악용할 수 있는 취약점이 남아 있는 시스템을 최소화할 수 있을 것이다.

둘째, AI 기반의 침입 탐지 및 예방 시스템을 연구하여 이터널블루와 같은 취약점을 실시간으로 감지하고 차단할 수 있는 기술을 개발할 것이다. 현재의 보안 시스템은 주로 기존에 알려진 취약점에 대해 패치를 적용하거나 차단하는 방식으로 운영되지만, 향후 연구에서는 패치가 적용되지 않은 취약점이나 알려지지 않은 취약점에 대한 실시간 탐지 및 대응 기술을 심화할 예정이다.

셋째, 보안 교육을 위한 실시간 시뮬레이션 환경을 구축하여, 학습자들이 이터널블루와 같은 취약점에 대해 보다 실질적으로 대응할 수 있는 훈련을 받을 수 있도록 할 것이다. 이를 통해 보안 담당자들이 실제 공격 상황에서 대응하는 능력을 배양하고, 시스템 방어 전략을 보다 효과적으로 구축할 수 있는 기반을 마련할 수 있을 것이다.

이를 통해 이터널블루와 같은 고위험 취약점에 대해 보다 효과적이고 포괄적인 대응 방법을 제시할 수 있으며, 사이버 보안 실습 환경 또한 더욱 발전시킬 수 있을 것이다.

# 참고문헌

**[참고문헌]**

[1] Luay A. Wahsheh, Biruk Mekonnen, "Practical Cyber Security Training Exercises," presented at the IEEE Computer Society Conference on Cybersecurity, 2019, pp. 48.

[2] 이용필, 김태성, 유진호, "국내 사이버 침해사고의 경제적 피해 금액 산정," Korea Business Review, 24(2) (2020): 1.

[3] H. Eck, "Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection," 2021 International Conference on Information Security and
Cryptology (ISCTURKEY), Ankara, Turkey, 2021, pp. 87-92, doi: 10.1109/ISCTURKEY53027.2021.9654331.
https://ieeexplore.ieee.org/document/9654331

[4] Gupta, M. R., Koli, Y. P., Patiyane, V. A., & Wagh, K. P. Eternal Blue Vulnerability.

[5] B. Fiore, K. Ha, L. Huynh, J. Falcon, R. Mendiola and Y. Li, "Security Analysis of Ransomware: A Deep Dive into WannaCry and Locky," 2023 IEEE 13th
Annual Computing and Communication Workshop and Conference

(CCWC), Las Vegas, NV, USA, 2023, pp. 285-294, doi: 10.1109/CCWC57344.2023.10099114. [6] \
[6] https://ieeexplore.ieee.org/document/10099114

[7]https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/

[8] A. D. Widegap and Y. Dewi Ward Hana Aznar, "Integrated Exploit Kit for Web Application," 2019 International Conference on Electrical Engineering and
Computer Science (ICECOS), Bantam, Indonesia, 2019, pp. 299-302, doi: 10.1109/ICECOS47637.2019.8984449.
https://ieeexplore.ieee.org/document/8984449

[9] 김승우. "자율주행차량과 AI 드론봇에 대한 해킹 공격 및 취약점 보안 연구." 국내박사학위논문 호서대학교 벤처대학원, 2020. 충청남도 115p.

[10] https://continuetochallenge.tistory.com/17

# 부록

[시연영상 QR코드,링크]

https://youtu.be/7hKs23Re5CA?si=ImQNIlWK4Eosq4Tu