Penetration Test Report

CyberPatrol inc

bernard (jong hyun) lee

2020

# Disclaimer

This report is written based on the penetrating test result under Virtual Machine environment with Kali Linux 2019.04 and Ubuntu installed. The test used the vulnerability of WordPress services to get initial credential and used hydra command to get the id and password. After getting an account to access, used poor security practice of root privileged nmap running to access root. The outline of this report comes from *“Writing a Penetration Testing Report.”*[[1]](#footnote-1)

# Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Description | Author | Approved by |
| 1.0 | 04-08-2020 | Initial version | Bernard Lee |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

All printed copies are valid only if the approver gives a written permission to print under his signature.

Table of Contents

[Disclaimer 1](#_Toc37243131)

[Version Control 1](#_Toc37243132)

[1. Executive Summary 3](#_Toc37243133)

[1.1. Scope of Work 3](#_Toc37243134)

[1.2. Summary of Results 3](#_Toc37243135)

[1.3. Assumption 3](#_Toc37243136)

[2. Attack Flow 4](#_Toc37243137)

[2.1. Gathering information 4](#_Toc37243138)

[2.2. Vulnerability check and get initial access to the target server 4](#_Toc37243139)

[2.3. Gathering further information to get a privilege access 6](#_Toc37243140)

[3. Conclusion 9](#_Toc37243141)

[4. Recommendation 10](#_Toc37243142)

[5. Risk Rating 10](#_Toc37243143)

# Executive Summary

This report is the result of a penetration test with controlled environment. All activities were conducted under the written permission and the ways that a hacker usually did. Through this test, CyberPatrol Inc. gives the customer the following result of:

* Identifying if the target system is vulnerable
* Identifying if the target system is cracked through finding vulnerabilities

CyberPatrol conducted the penetration test based on the vulnerability of existing services, got privileged access by using vulnerability of poor administration practice of nmap having permission 4000 which means that the command has root privilege while it is executing. We could get root access by executing the command, nmap --interactive. Through this test, vulnerabilities of software gave us the key to open the door, and insecure practices helped us to get full access of the server.

## 1.1. Scope of Work

The test was designed to do following steps within a virtual environment.

* Scanning target network to find a victim (server)
* Getting detail information about the victim (server)
* Using vulnerability of the services
* Using hydra to gather id and password
* Accessing WordPress to modify 404.php.
* Getting access the victim by appending php-reverse-shell.php at the end of the file 404.php.
* Accessing the victim using nc command and connect
* Using find / -perm -4000 to check possible attack options
* Executing nmap –interactive to have a root privilege
* Getting root privilege through namp interactive mode

## 1.2. Summary of Results

The test used Word Press vulnerability to get ids and got passwords from hydra command. After that, we could get login id and password, so we accessed the server to go further. Through modifying 404.php, we could connect the target by using nc command. Finally, we could get root privilege by executing nmap –interactive command.

## 1.3. Assumption

Firstly, the written permission to a penetration test is issued and approved. Secondly, the target server is not on real service status and has a duplicate copy on a virtual environment. Thirdly, the server has vulnerable services. Fourthly, the tester uses Kali Linux on the same virtual network to test. Lastly, this report is only valid under this controlled test condition only and if something is changed, the result may be different.

# Attack Flow

## 2.1. Gathering information

Gathering information is the first step of our penetration test, so we use nmap command to scan the target network 192.68.56.0/24. We can find the target system’s IP address (192.168.56.111) and three services ssh, http, and https. We could find the detail of the service by specifying argument “-p<start port number>-<end port number>” or “-p<port number>.” Similarly, all services at the server, 192.168.56.110, can be scanned with option “-sV -O 192.168.56.110 -p1-65535” where 1 is the start port number and 65535 is the last port number. For your information, we do not need to scan all ports as we knew only three services were on the server

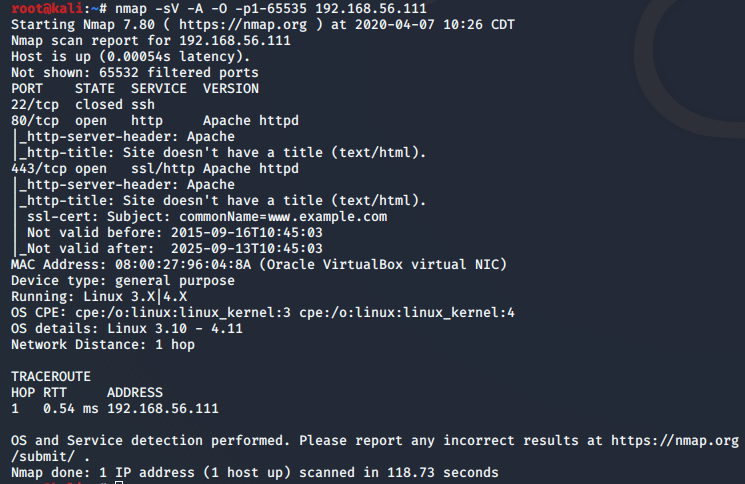
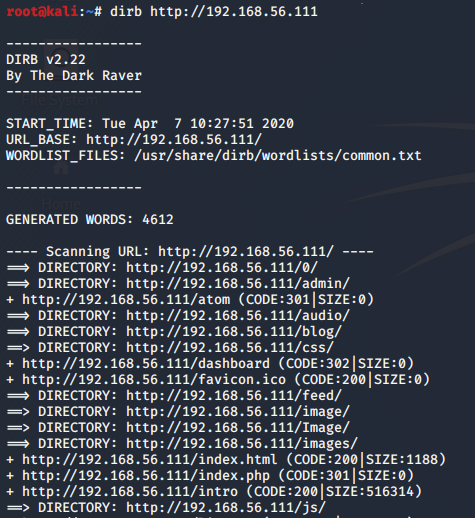


Figure nmap scan result. nmap -sV -A -O -p1-65535 192.168.56.111

## 2.2. Vulnerability check and get initial access to the target server

First of all, from the detailed scan, we can find http service so we can use dirb and nikto (dirb <http://192.168.56.110> and nikto -h http://192.168.56.111) to gather some information.. The following pictures show the result of executing dirb and nikto:



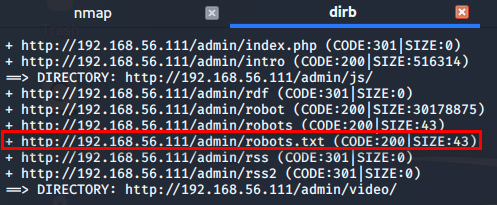


Figure dirb http://192.168.56.111

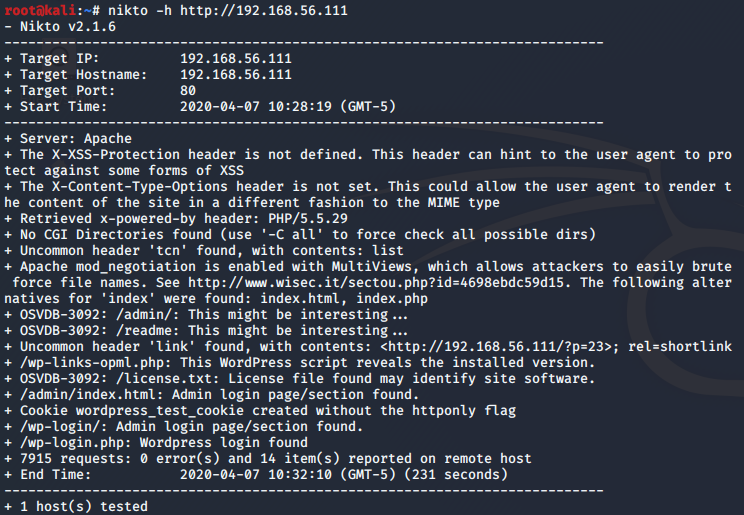


Figure nikto -h http://192.168.56.111

We check the web site from dirb’s result and we could download fsocity.dic file from the victim server to get some hints for getting a id and the password of the id.

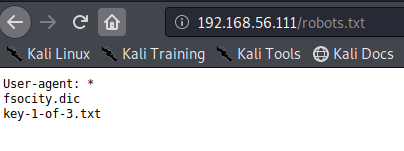


Figure Some information from the victim

Similarly, we used hydra command for a id and the password of the id and we could get the id, elliot, and the password, ER28-0652. The following pictures show the result of getting a id and the password

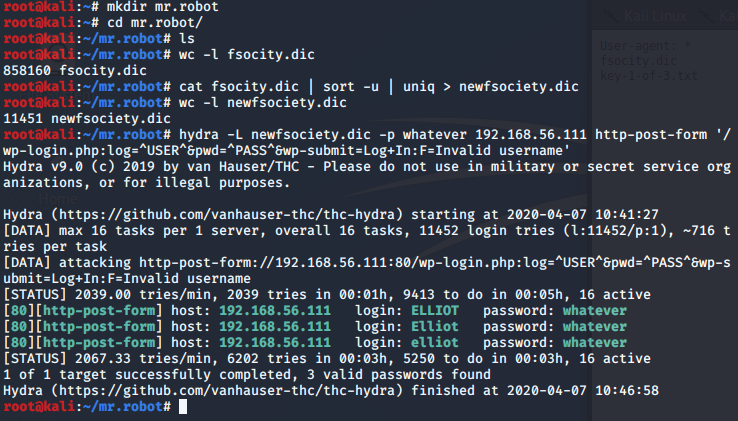


Figure getting a user id using hydra command using dictionary from the victim

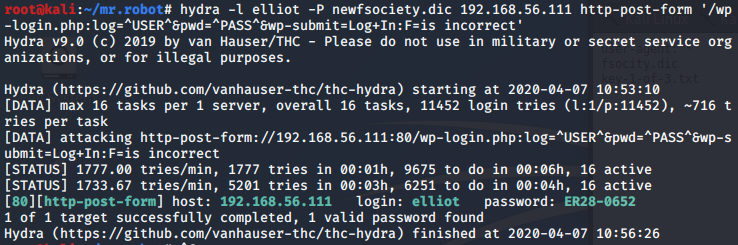


Figure getting password using hydra

## 2.3. Initial access to connect the server with reverse shell

First of all, after getting the passwords, we could connect the target through Word Press login page <http://192.168.56.111/wp-login> with the id, elliot, and the password ER28-0652 from hydra result.

Next, we could access Word Press admin page and append reverse-shell code after 404.php file. The following picture show the append result.



Figure Append reverse-shell code after 404.php

Finally, we could connect to the target server by using nc -nvlp 1234

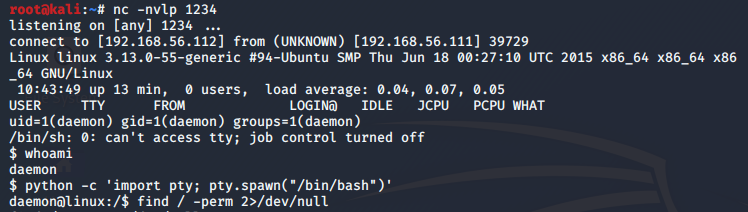


Figure Connect to the target using nc

# 2.4. Access root account

Finally, we could access to root privilege by using namp – interactive comand.

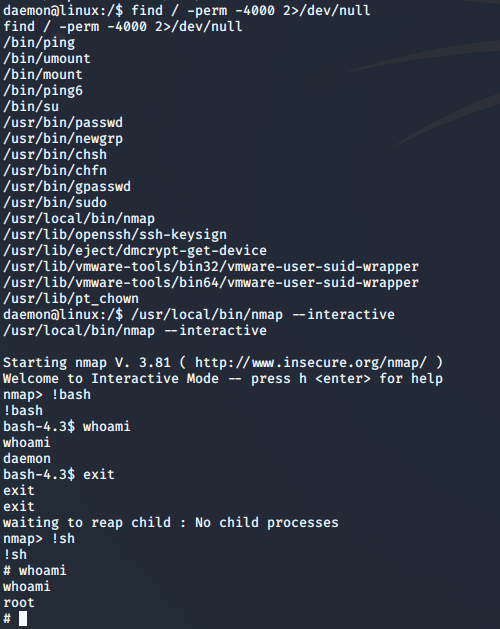


Figure Getting root privilege

# Conclusion

All activities were conducted under the written permission and the ways that a hacker usually did. All activities are conducted to simulate an unauthorized access from outside. Through this test, CyberPatrol Inc. gives the customer the following result of:

* The target system is vulnerable
* The target system is cracked through finding vulnerabilities

CyberPatrol conducted the penetration test based on the vulnerability of word press, and using some executable files with having root privilege during their execution. The test result shows that those poor practices led the hacker into the server.

# 4. Recommendation

Due to the limitation of the test scope, CyberPatrol could conduct penetration test on one server but another servers can have similar vulnerabilities. Based on our founding, we suggest several recommendations.

1. **Ensure to allocate proper resources to handle information system security.** The vulnerable servers are usually caused by lack of knowledgeable staff. Knowledgeable staff and enough time to handle security issues can make big differences than your company expects.\
2. **Setup processes to handle security issues.** Most of unauthorized accesses use vulnerable report to get an access. Manual checking can be a great solution but not enough to mitigate all risks. Setting automated processes are very effective to prevent without missing vulnerabilities.
3. **Implementing patch management system.** Patching servers are most common way to minimize the vulnerabilities of servers. Good resource for patch management system can be found at SP 800-40 Rev. 3[[2]](#footnote-2).
4. **Disable unnecessary services.** Disabling unnecessary services is the fastest way to mitigate current security issues. Allowing minimal access to the server is the great way to enhance security.
5. **Conduct regular vulnerability assessment.** SP 800-30 Rev. 1[[3]](#footnote-3) is a good resource to reference. Conducting risk assessment regularly is a part of risk management of a company. Also ISACA COBIT 2019[[4]](#footnote-4) is another good source to refer.

# 5. Risk Rating

The overall risk identified to the system as a result of the test is high. It is reasonable to believe that an unauthorised attacker can gain the system access any time based on the penetration result.

1. Mansour A. Alharbi, SANS Institute InfoSec Reading Room - Writing a Penetration Testing Report, April 6, 2010 [↑](#footnote-ref-1)
2. <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final> [↑](#footnote-ref-2)
3. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final> [↑](#footnote-ref-3)
4. <https://www.isaca.org/resources/cobit> [↑](#footnote-ref-4)