****

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY 2015

IT 501 - Information and Network Security

Assignment 01 – Year 1 Semester 2

Lecturer: Mr.Lakmal Rupasighe

**Bug Bounty-Progress 2**

S.S.Niranga - MS14901836

# Abstract

A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-users’ adherence to security policies.[[1]](#endnote-1)

# Acknowledgement

I would like to express my special thanks of gratitude to Dr. Samantha Thelijjagoda for providing me with the opportunity to study at SLIIT as well as my Mr.Lakmal Rupasinghe who gave me this golden opportunity to do this assignment on the topic "Security and penetration testing", which also helped me in doing a lot of research and I came to know about so many new things and I am really thankful to them. Secondly, I would also like to thank wife and friends who helped me a lot in finishing this project within the limited time.

I am making this assignment not only for marks, but to also increase my knowledge.

Thanks again to all who helped me.

Table of Contents

[Abstract 2](#_Toc414563113)

[Acknowledgement 3](#_Toc414563114)

[Progress 2 5](#_Toc414563115)

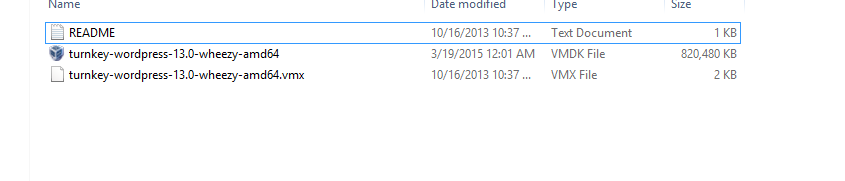
[**Detecting OpenSSL-Heartbleed with nmap** 5](#_Toc414563116)

[References 8](#_Toc414563117)

# Progress 2

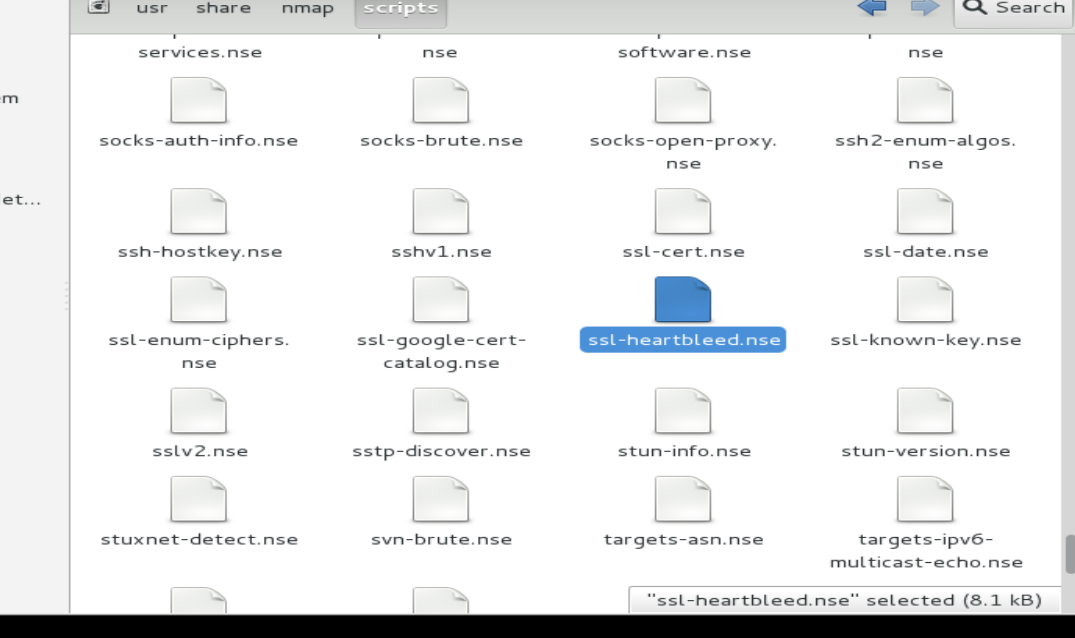
## **Detecting OpenSSL-Heartbleed with nmap**

Download VM from <http://www.turnkeylinux.org/wordpress>



Once the WordPress VM was configured, I then fired up my Kali Linux VM.

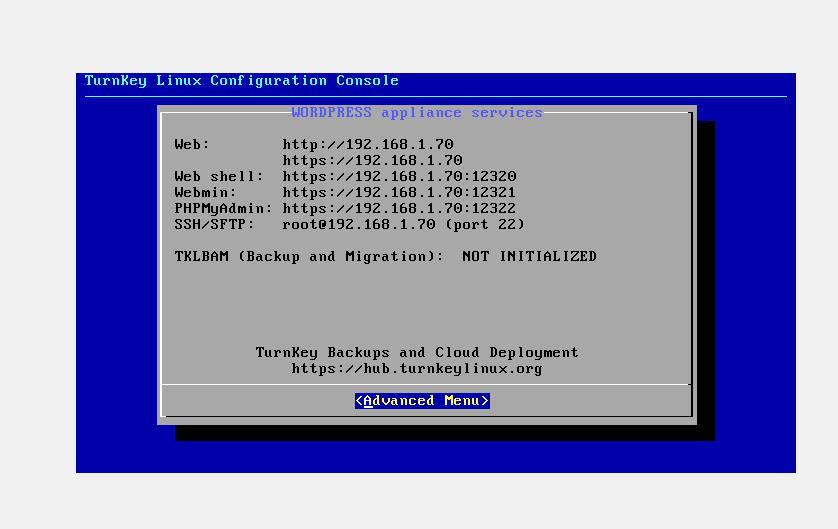
The I have visited to kali linux and check the availability of <https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse>



Then I have checked the “tls.lua” library file. If it’s unavailable download.

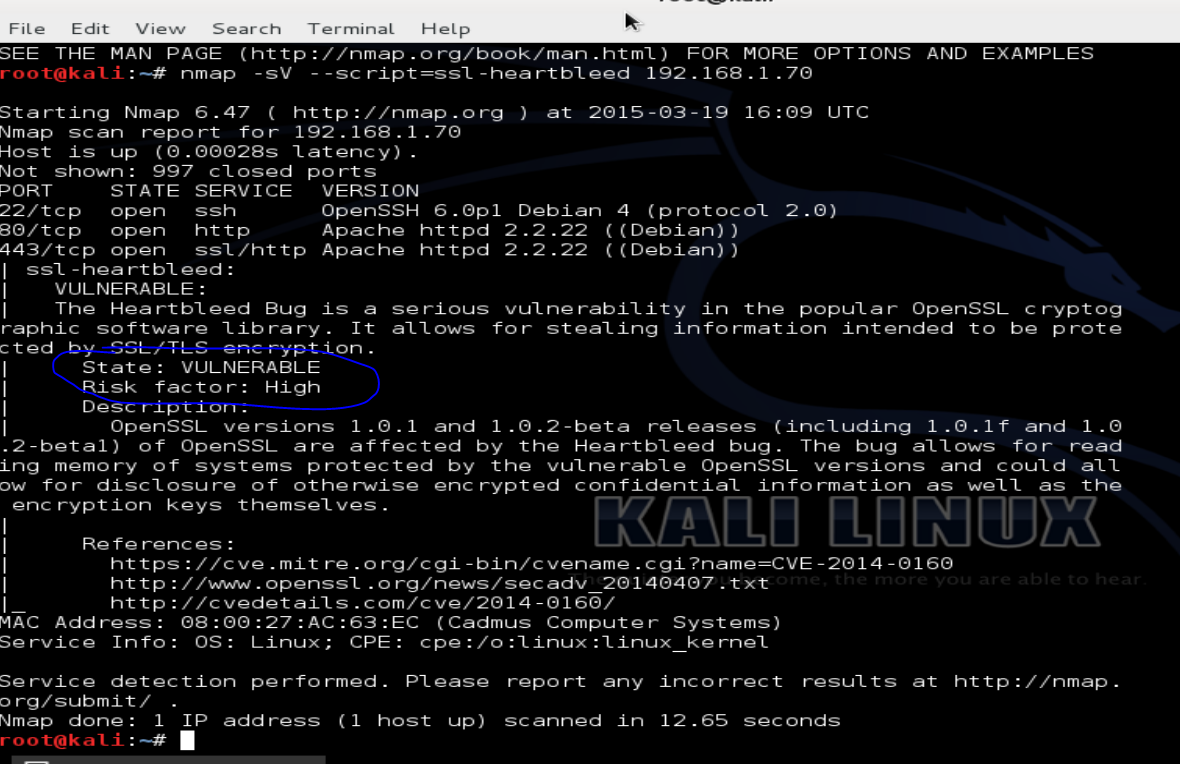


After this, I have ran the WordPress VM and followed the instruction and setup the VM.



After completing this, I have executed below command in kali

**nmap -sV --script=ssl-heartbleed 192.168.1.70**



It has retuned,

State : VULNERABLE

Risk Factor : High

That means this server is vulnerable.

# References

1. <http://www.coresecurity.com/penetration-testing-overview> [↑](#endnote-ref-1)