

A study of Security Vulnerabilities Within a Private Virtual Environment

Thomas Barnett (1902040)

BSc Computer Networks and Cybersecurity

Introduction

Cyber-Attacks have become an ever more increasing challenge to overcome in the past few years. These challenges can be very hard to battle with and keep under control. Therefore, having system in place to keep you safe from future cyber attacks will allow for a more secure system. Within this project there are multiple penetration tests done through a simulated system to replicate a cyber attack that can occur at anytime. Running these tests allows for the research of vulnerabilities in the system and flaws. These flaws can then be fixed to make the system more secure. Allowing for less cyber attacks being successful.

Software's Used

- Oracle Virtual Box
- Kali
- Metasploit Framework
- Metasploitable 2
- Nmap
- Nessus



Hypothesis

Vulnerabilities are exploited less on secure system

Null Hypothesis

Vulnerabilities are exploited more on a non-secure system

Conclusion

Running these exploits has allowed for a better understanding of cyber-attacks and the methods to limit the attack surface. It has also shown the different software useable to create your own penetration test

Future work

Within the future of this project, I would exploit more ports and fix and harden possible flaws to stop these exploits.

Results

Exploits	Exploited	Failed
Exploiting Port 80 HTTP		
Exploiting Port 22 SSH		
Exploiting Port 23 Telnet		
Exploiting Port 21 FTP		
Exploiting Port 25 SMTP		
Exploiting Port 139 445 SMB		
	Exploited	Failed

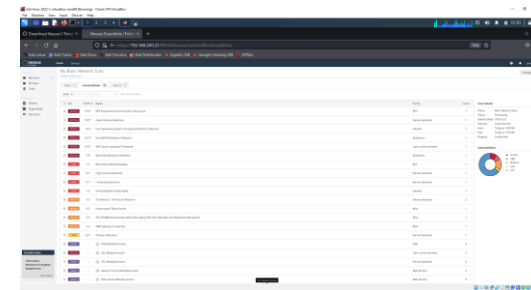
Experiment

Nmap.

Nmap will be used to scan the Metasploitable2 host for open ports.

Vulnerability Analysis: (Nessus).

Utilising Nessus to scan for vulnerabilities that can be exploited



Exploitation.

Several common vulnerable ports were chosen and subjected to vulnerability scanning in order to remotely exploit the attack surface. These included, 80(HTTP), 22(SSH), 23(Telnet), 21(FTP), 25(SMTP) and 139/445(SMB)

Contact Information: tom.barnett99@gmail.com