

To Identify vulnerabilities of the local network by pen testing and mitigating the vulnerabilities by enhancing the security

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 to test the vulnerabilities found within the Nessus scan. These penetration tests were then given mitigations to improve or stop future attacks..

This paper has the involvement of an experiment conducting penetration tests on proven vulnerabilities to find mitigations for said vulnerabilities. These penetration tests are done through a multitude of software working with each other. Software's such as Kali Linux, Metasploit Framework, Metasploitable 2, Nessus and Nmap. Each software is used to conduct said pen test within experiment section of paper. Within this paper there is information on said software's above and academic literature on proven techniques of penetration tests using software's talked about above.

Software's Used

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



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:

Each test was successful and followed each expected outcome:

Here is the expected outcome of VNC server "password" exploit. This exploit is the one showed within this poster.

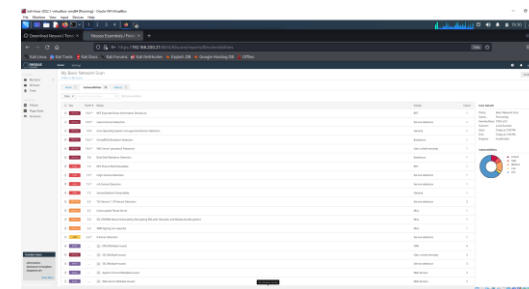
VNC Server Password:

depicts access to the VNC server using the disclosed 'password' as a password." And further below paragraph "To learn more about the attack, a vnc shell is used to connect to the MySQL server and then dump one of the databases

Experiment

Vulnerability Analysis: (Nessus).

Utilising Nessus to scan for vulnerabilities that can be exploited



Exploits:

Samba MS-RPC
PHP CGI Argument Injection
VSTFPD Backdoored
Java RMI Server Code Execution
UnrealRCD Backdoored
VNC Server "password"

VNC Server "password" Exploit:

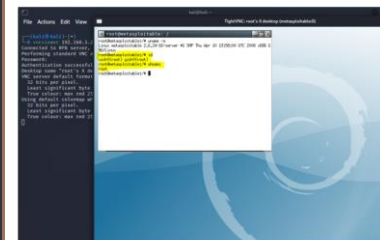


Figure 11 VNC server access

Mitigation

- Strong secure password creation with the following rules:
- The password should not RESEMBLE the username, nor vice versa.
- Every password must contain at least one letter, one number, and one special character, and there must be a mix of upper- and lower-case letters.
- The password should be long enough.

To learn more about the attack, a vnc shell is used to connect to the MySQL server and then dump one of the databases, as seen in figure 12 below.



Figure 12 MySQL server

Contact Information: tom.barnett99@gmail.com