Penetration Testing for FCM 745—Michael Fernez

I. Executive Summary

Our class was tasked with a sample penetration test on servers set up at John Jay College by Professor Obaidat.

The goals of this penetration test are as follows:

1) to identify if an attacker can compromise the Ubuntu Server in question at IP 10.5.62.84
2) determine the impact in the event the system is compromised on
    a) confidentiality and integrity of system information
    b) availability of the server

Penetration testing was conducted following the specifications in NIST SP 800-115 with recommendations from the InfoSec Institute [1] and Offensive Security [2].

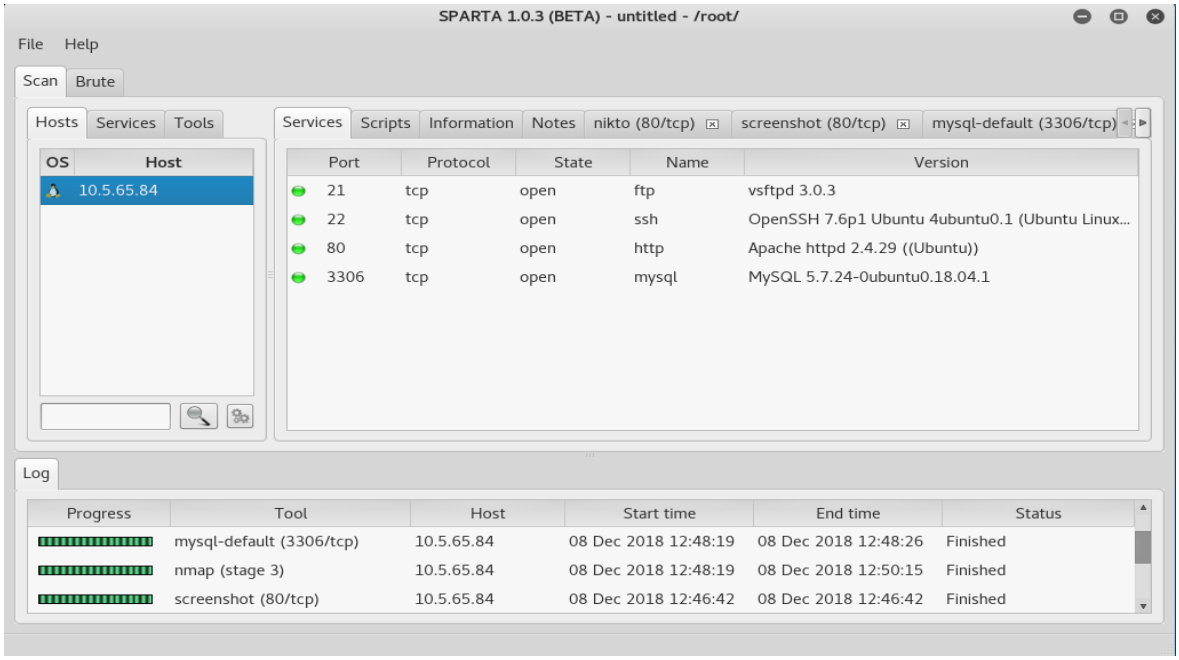
A. Summary of Results

II. Vulnerability Analysis

A. Vulnerability Scans with Nmap and Nikto

Given a specific host to probe host was discovered using Nmap and analyzed further with a Sparta vulnerability scan, which utilized nmap, nikto, and various connection services.

The result revealed ftp, ssh, apache, and mySQL services running on ports 21, 22, 80, and 3306 respectively.

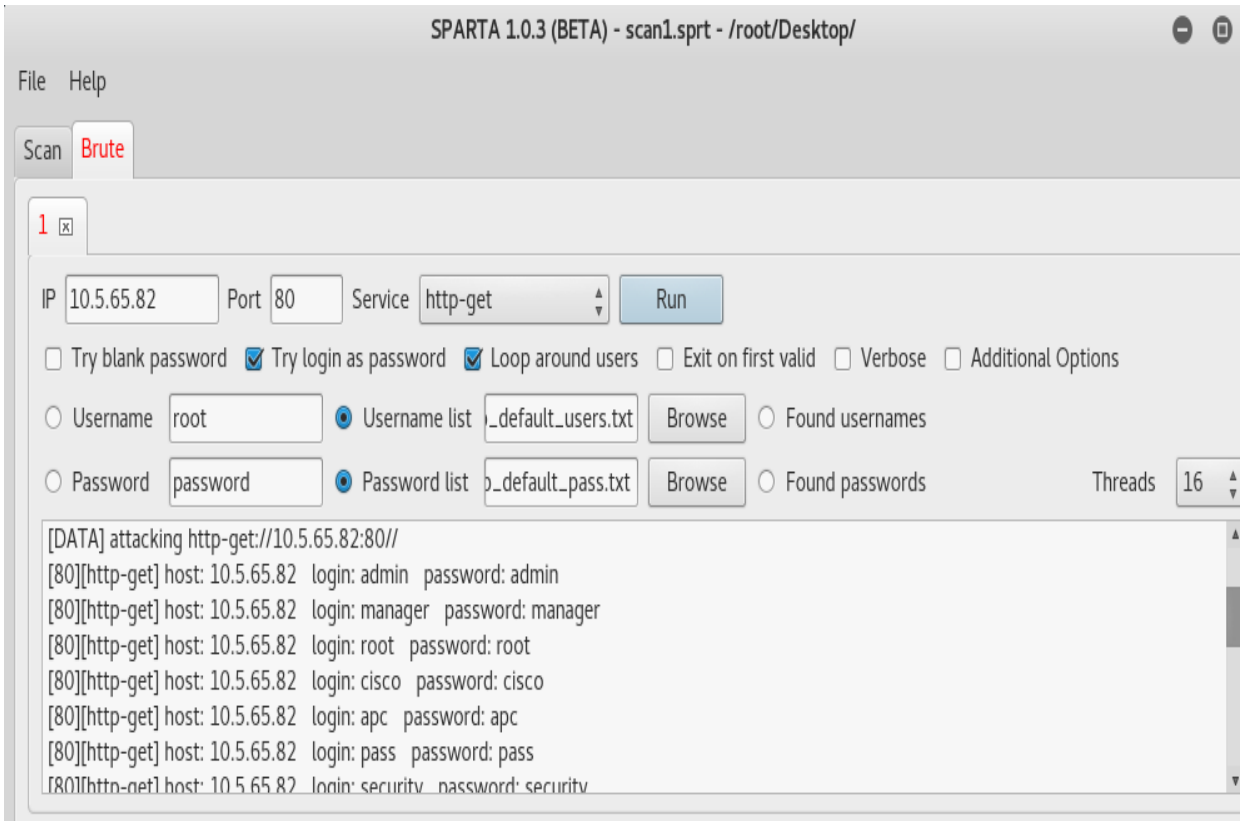


B. Brute Force Connection attempts

Following the Sparta scan, I attempted to brute force each connection using the default word lists provided by metasploit utilizing the “Brute” tab in Sparta.

i. Apache Server

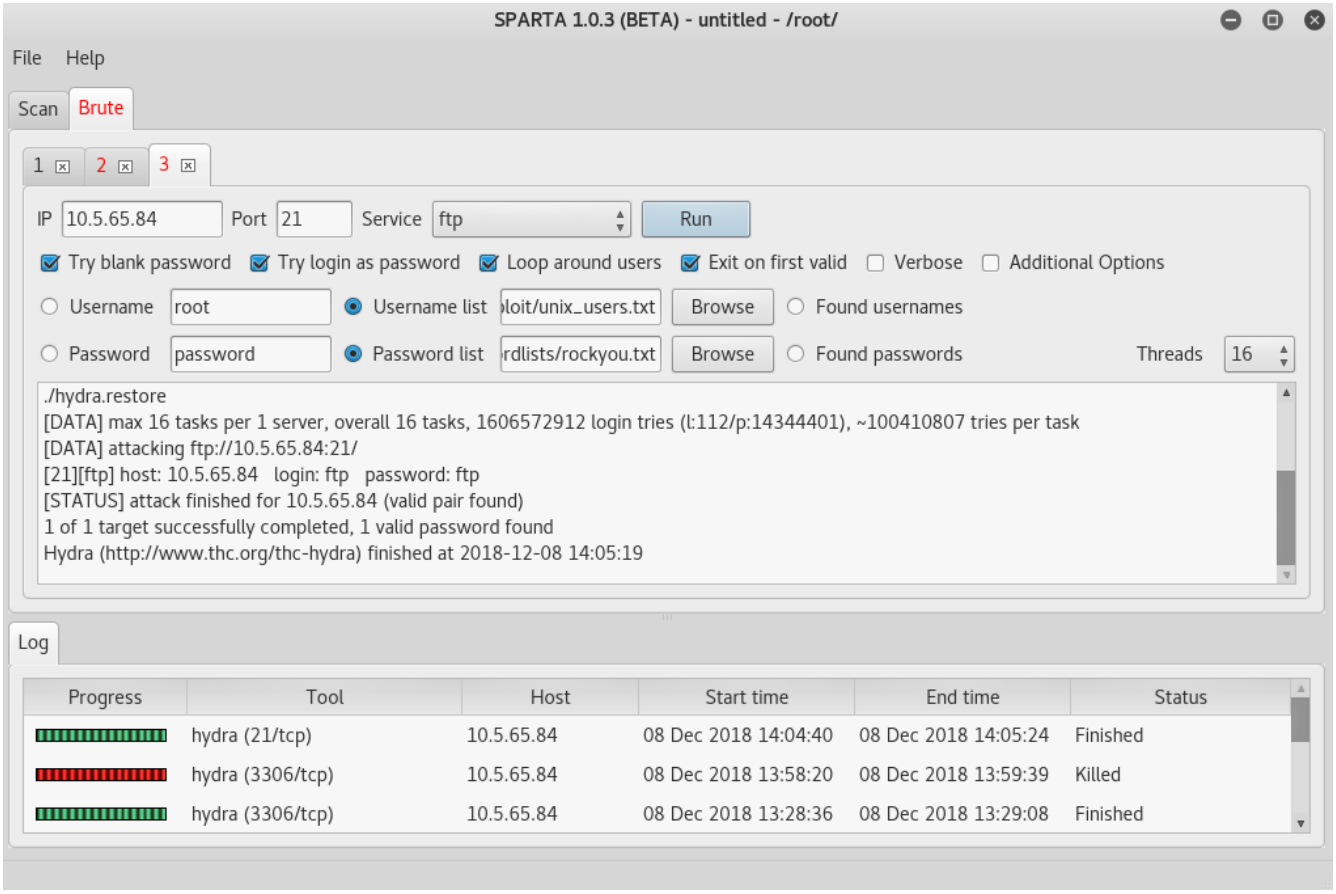
Entering the IP address in a browser reveals the default Apache2 Ubuntu page, suggesting that this server may be using default passwords and usernames Using the http_default_pass and users files with THCHydra via Sparta revealed the site is using several default usernames and passwords



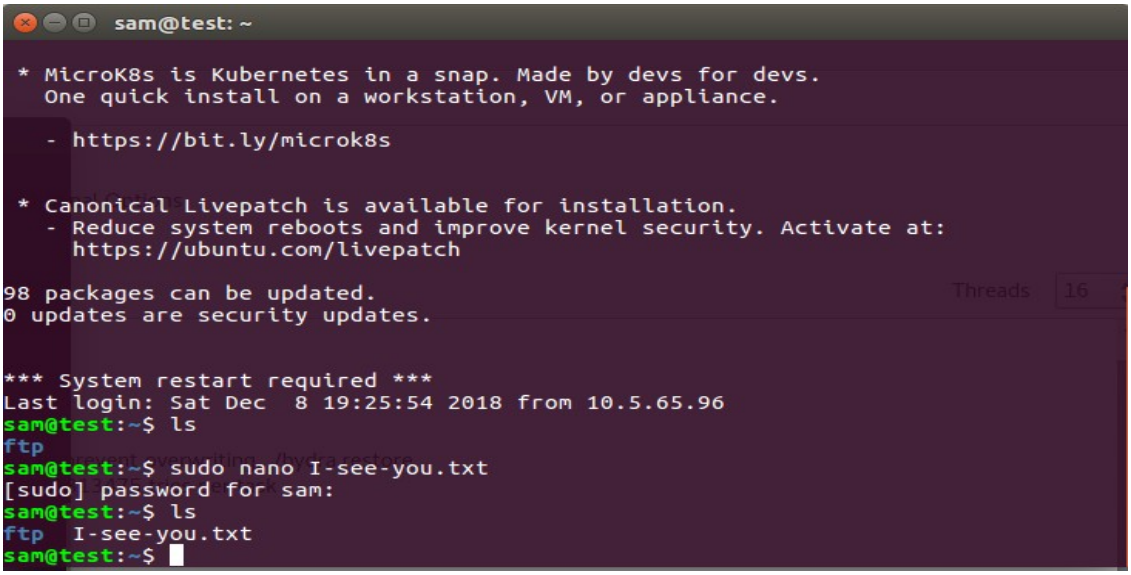
Using the tomcat default lists additional logins were revealed, detailed in Appendix A. (Note: IP is different here because the test was conducted before the new server was in place. A second test confirmed the logins were still valid on the 10.5.62.84 server)

ii. FTP and SSH Server

Using a publicly available password list and cycling through the default unix_users list, the login to the ftp serve was found relatively quickly. It was found this account could read files on the server and even transfer files to the server (such as simple text files).

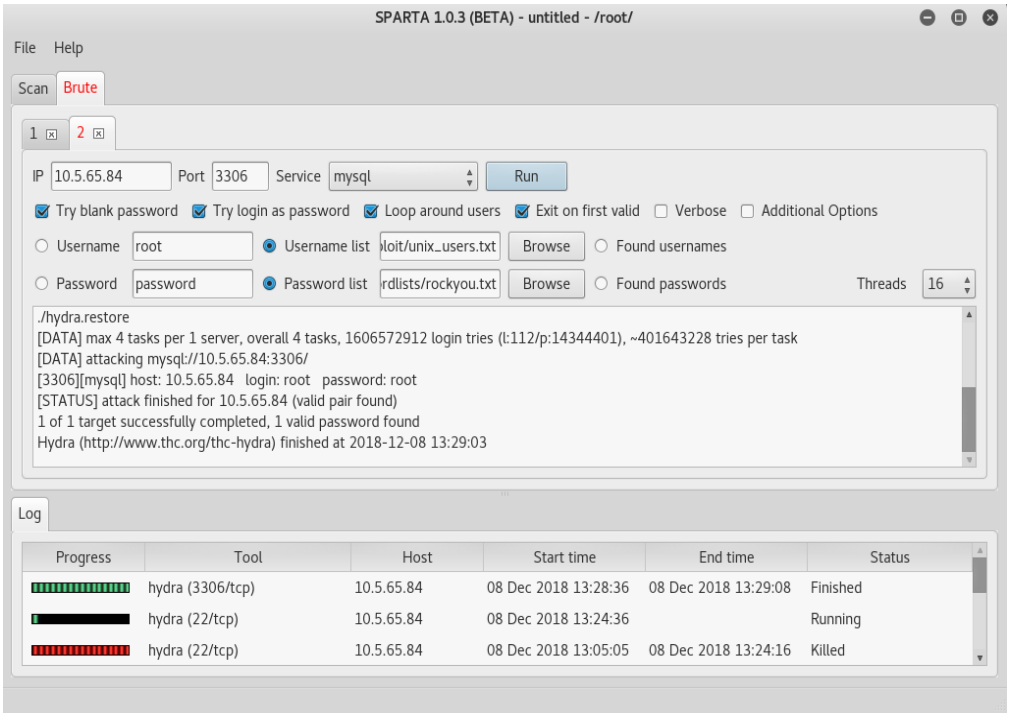


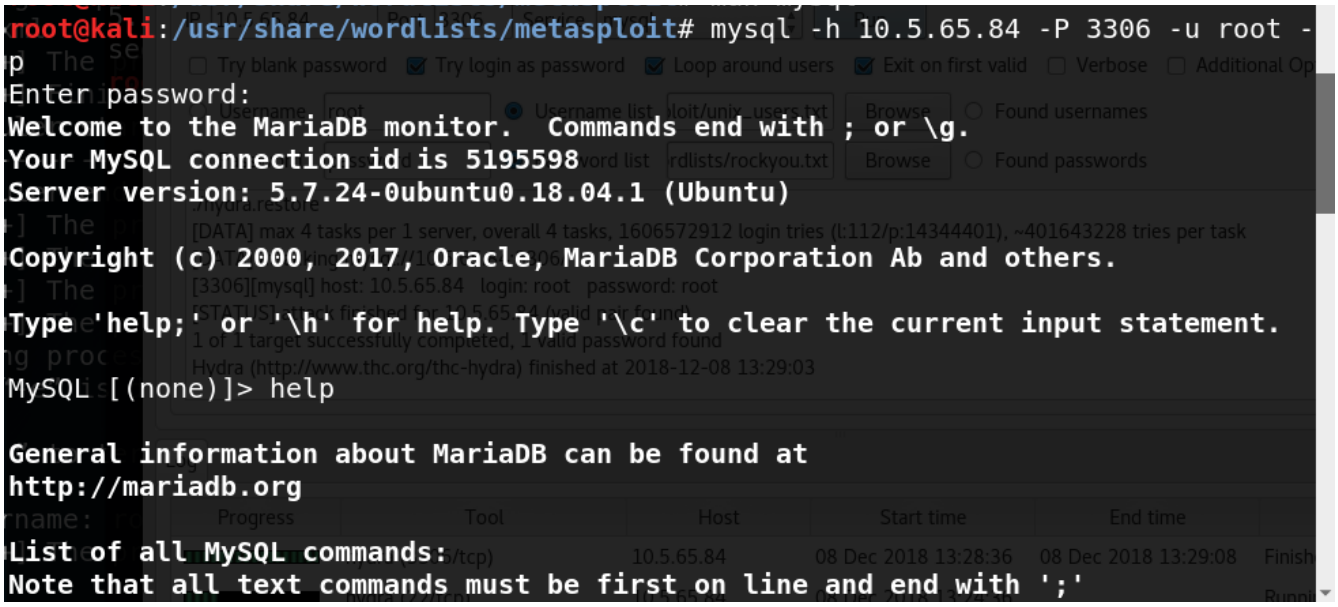
The ssh server proved to be a more time-consuming task, but using the password list as the username list as well eventually found a username, “sam,” using an easily guessable password. It was found this user has root privileges and can read and write files at will.



iii. MySQL database

Using the same method as the FTP brute force, the login to the SQL server was found very quickly as it is currently using a default username and password. With this login, a user can execute arbitrary SQL commands to read, write, and delete data from the server.





III. Classification of Vulnerabilities and Recommendations

Vulnerability: SSH Login with weak password

Risk: Critical

Impact: A user with access to this SSH server can read and write files and execute programs. Since the account found has root privileges, an attacker who finds it has full access to the machine.

Remediation: Revoke Sam's root privileges and/or have him change both the username and the password. A user's account should never have a password that matches the username, especially one so easily guessable with publicly available word lists. Passwords should be at least 15 characters in length containing a combination of letters, numbers and special characters.

Vulnerability: SQL databse login with default credentials

Risk: High

Impact: A user with access to this MariaDB server can execute SQL commands that read, write, and drop tables from the SQL database. This can potentially compromise other systems if the databases contain account info.

Remediation: Disable default logins and considering disabling the database if it is not being used.. Default usernames passwords are a common vulnerability on fresh installations of MariaDB. It is recommended that each user have a unique username and password, with passwords at least 15 characters in length containing a combination of letters, numbers and special characters.

Vulnerability: FTP Login with default credentials

Risk: Medium

Impact: A user with access to this FTP server can read and transfer files on the server. This could enable an attacker to read sensitive data, change sensitive data, and transfer malicious executables to the server.

Remediation: Change both the username and the password. Default usernames passwords are a common vulnerability on fresh installations of FTP. It is recommended that each user of the FTP server have a unique username and password, with passwords at least 15 characters in length containing a combination of letters, numbers and special characters.

Vulnerability: Apache Login with default credentials

Risk: Medium

Impact: A user with access to this web server can make changes to webpages and read potentially sensitive data.

Remediation: Disable default logins and limit the users who can access the server and change the Apache default webpage. Default usernames passwords are a common vulnerability on fresh

installations of Apache. It is recommended that each user have a unique username and password, with passwords at least 15 characters in length containing a combination of letters, numbers and special characters.

IV. Appendix A: Tools Used and References

Kali Linux Penetration Testing OS
Sparta – Comprehensive Vulnerability Suite using nmap and nikto
Nikto – Vulnerability scanner
Nmap – port scanner
Metaploit – Penetration Testing Framework
Password lists from https://wiki.skullsecurity.org/Passwords

1. https://resources.infosecinstitute.com/writing-penetration-testing-reports/
2. https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

V. Appendix B: Login Credentials for Apache Web Server

[80][http-get] host: 10.5.65.82 login: admin password: admin
[80][http-get] host: 10.5.65.82 login: manager password: manager
[80][http-get] host: 10.5.65.82 login: root password: root
[80][http-get] host: 10.5.65.82 login: cisco password: cisco
[80][http-get] host: 10.5.65.82 login: apc password: apc
[80][http-get] host: 10.5.65.82 login: pass password: pass
[80][http-get] host: 10.5.65.82 login: security password: security
[80][http-get] host: 10.5.65.82 login: system password: system
[80][http-get] host: 10.5.65.82 login: sys password: sys
[80][http-get] host: 10.5.65.82 login: wampp password: wampp
[80][http-get] host: 10.5.65.82 login: newuser password: newuser
[80][http-get] host: 10.5.65.82 login: manager password: admin
[80][http-get] host: 10.5.65.82 login: user password: user
[80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: xampp-dav-unsecure
[80][http-get] host: 10.5.65.82 login: vagrant password: vagrant
[80][http-get] host: 10.5.65.82 login: root password: admin
[80][http-get] host: 10.5.65.82 login: cisco password: admin
[80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: admin
[80][http-get] host: 10.5.65.82 login: vagrant password: admin
[80][http-get] host: 10.5.65.82 login: user password: password
[80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: password
[80][http-get] host: 10.5.65.82 login: vagrant password: password
[80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: manager
[80][http-get] host: 10.5.65.82 login: vagrant password: manager
[80][http-get] host: 10.5.65.82 login: user password: admin
[80][http-get] host: 10.5.65.82 login: xampp-dav-unsecure password: letmein

[80][http-get] host: 10.5.65.82 login: vagrant password: letmein

[80][http-get] host: 10.5.65.82 login: manager password: manager
[80][http-get] host: 10.5.65.82 login: root password: admin
[80][http-get] host: 10.5.65.82 login: role1 password: manager
[80][http-get] host: 10.5.65.82 login: role1 password: role1
[80][http-get] host: 10.5.65.82 login: manager password: admin
[80][http-get] host: 10.5.65.82 login: role1 password: admin
[80][http-get] host: 10.5.65.82 login: tomcat password: admin
[80][http-get] host: 10.5.65.82 login: both password: admin
[80][http-get] host: 10.5.65.82 login: admin password: manager
[80][http-get] host: 10.5.65.82 login: both password: manager
[80][http-get] host: 10.5.65.82 login: admin password: admin
[80][http-get] host: 10.5.65.82 login: root password: root
[80][http-get] host: 10.5.65.82 login: tomcat password: tomcat
[80][http-get] host: 10.5.65.82 login: root password: manager
[80][http-get] host: 10.5.65.82 login: tomcat password: manager
[80][http-get] host: 10.5.65.82 login: both password: both
[80][http-get] host: 10.5.65.82 login: admin password: role1
[80][http-get] host: 10.5.65.82 login: tomcat password: role1