PERFORMANCE ANALYSIS OF PASSWORD ATTACKING TOOLS

Saad Ghani, Tyrik Emptage, Kardish Mounie, Aparicio Carranza

Computer Engineering Technology

19th Annual City Tech Poster Session

ABSTRACT

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, one of which is password attack. This Operating Systems (OS) is used by many people for hacking and for exploiting security breaches. Kali Linux provides many built-in tools that can be used to breach security measures of different devices. We have experimented with the following tools: "Hydra", "John the Ripper", and "Findmyhash" as password attack applications. We report the performance analysis and evaluation of the above-mentioned tools indicating how well each goal is accomplished for the designated task

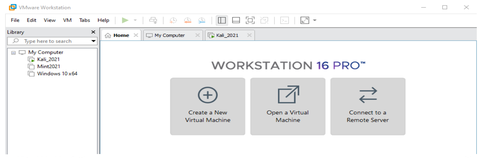
INTRODUCTION

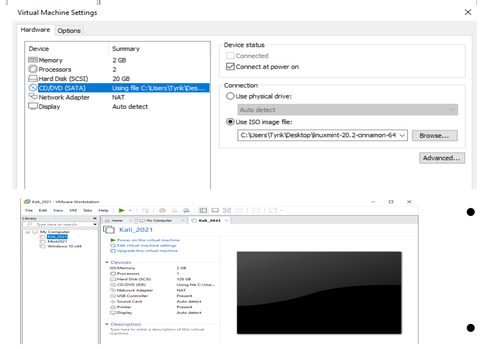
- **The purpose of this project is to analyze how well different tools complete the task.**
- **We will go over the fundamentals of Kali Linux and how it is used.**
- **We will explain each of the three different tools that are going to be used: "Hydra", "John the Ripper" and "Findmyhash".**
- **We will then explain the parameters that are going to be used when comparing the performance of each of the tools.**
- **After obtaining our results, we will determine which of the tools is best suited for password attacks, which method is the best, and how the tools affects the system it is being ran on.**

IMPLEMENTATION/TOOLS

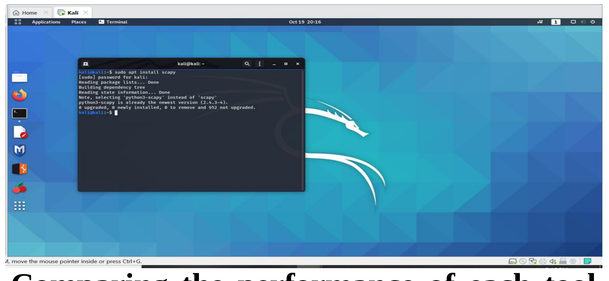
VIRTUAL MACHINE SETUP

- **Installing VMware**
- **Installing Linux OS Kali**
- **Creating a new virtual machine**
- **Downloading the iso file**
- **Power on the virtual machine**



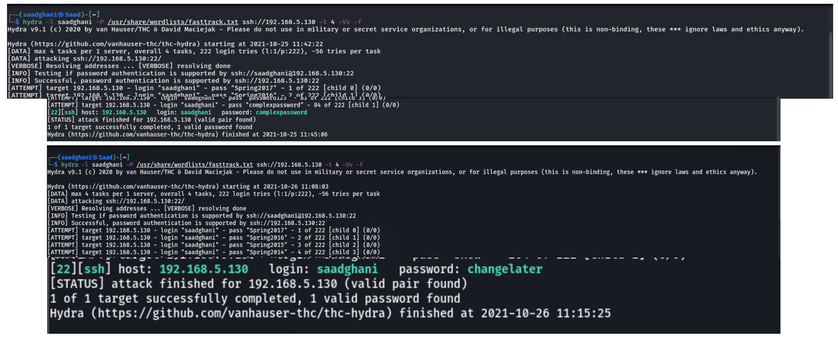


METHOD



- **Comparing the performance of each tool at completing their task**
- **THC Hydra -**
  Most protocol coverage, very fast and flexible
- **John the Ripper -**
  Can combine the data in different text files and hashes, compatible with windows
- **Findmyhash -**
  Has empty hash recognition, cracks single or multiple hashes and can hash search on Google

RESULTS



- **Current results show that it took Hydra 1'54" to crack a password after 84 attempts, and 7'22" to crack a password after 202 attempts**
- **Results on John the Ripper suggests that a password will take a longer time to crack if a wordlist is involved during a dictionary attack because the password from the user isn't in the wordlist**
- **The results for Findmyhash shows that the hash chosen wasn't listed on the online databases. Using the hasher function MD5 it showed that the string chosen couldn't be cracked**

CONCLUSION

- **General results based on observations so far**
- **CPU Usage data will be gathered**
- **Overall efficiency of each tool will be looked at**

REFERENCES

[1] Broad J. and Bindner A. (2013), *Hacking with Kali: Practical Penetration Testing Techniques*, Syngress

[2] Singh A. (2013), *Instant Kali Linux*, Packt Publishing

[3] *hydra | Kali Linux Tools*. (2021). Kali Linux. https://www.kali.org/tools/hydra/

[4] P. (2015, December 23). *THC-Hydra*. Penetration Testing Tools. https://tools.kali.org/password-attacks/hydra

[5] Baloch R. (2014), *Ethical Hacking Penetration Testing Guide*, Auerbach Publications