



Vulnerabilities and VMs

AU | Michael Edwards, Shawn Edwards, Michael Ford, Sean Hart

SRNL | Dillon Tauscher



SAVANNAH RIVER NATIONAL LABORATORY

Vulnerabilities/Threats | 3 MIN READ | PRODUCTS & RELEASES

1 in 3 Organizations Do Not Provide Any Cybersecurity Training to Remote Workers Despite a Majority of Employees Having Access to Critical Data

January 12, 2023



PITTSBURGH, Jan. 12, 2023 /PRNewswire/ -- New research from leading cybersecurity provider [Hornetsecurity](#) has found that 33% of companies are not providing any cybersecurity awareness training to users who work remotely.


"There is a cumulative impact here: You don't have enough people, the people you have don't have the right skills and the people that you have aren't getting the right training," Jon Oltsik, senior principal analyst at the Enterprise Strategy Group (ESG) on cybersecurity training.

Our Solution


- SRNL Cyber Awareness Training Module
- User-friendly application for cybersecurity training in vulnerabilities and exploits.
 - Step-by-step training modules curated for specific vulnerabilities by operating system.
 - Simple GUI for accessibility and modularity
 - Allowing inexperienced and veteran IT professionals to familiarize themselves with old and newer Operating systems
 - Teach these individuals how to exploit and remedy vulnerabilities on their machines

Design


Please select an exercise group to begin your training




Basics




Social Engineering



Web Applications



Kali Linux



Ubuntu




More




Kali-Linux Training Exercises

Man In The Middle Lab




Password Cracking Lab



Main Menu




Page 1



Man in the Middle Attack
With Kali Linux

In this lab we are going to demonstrate the basic concepts of an attack known as a Man in the Middle attack (MitM).



A man in the middle attack is an attack designed to intercept communication between a server and a client. We will be using Kali Linux to emulate a MitM attack using legitimate looking tools that Kali has to offer.

First thing we need to do is boot up our Kali Box and when it eventually gets to the login prompt:

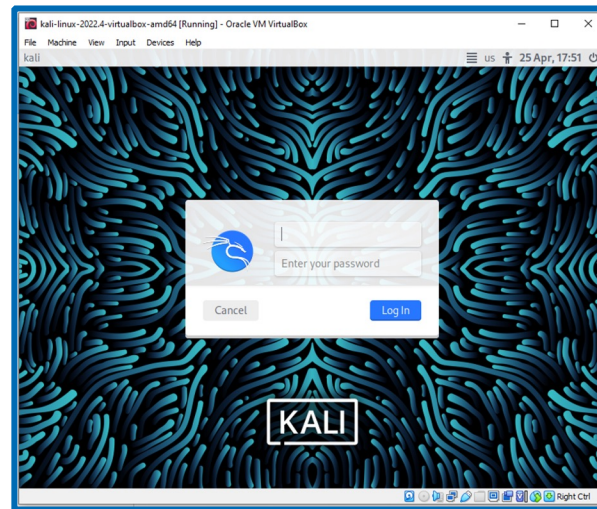
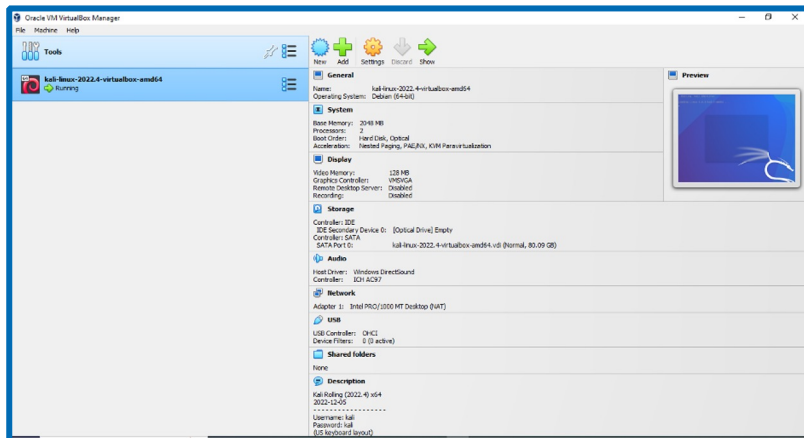
User: kali
Pass: kali

Boot VM

Quiz

Help

Menu



Pros/Cons

Pros

- Simple user interface
- Modular structure
 - Allows for easy implementation of additional lab exercises
- Thorough documentation
 - background information on the desired subject
 - step-by-step approach to minimize confusion

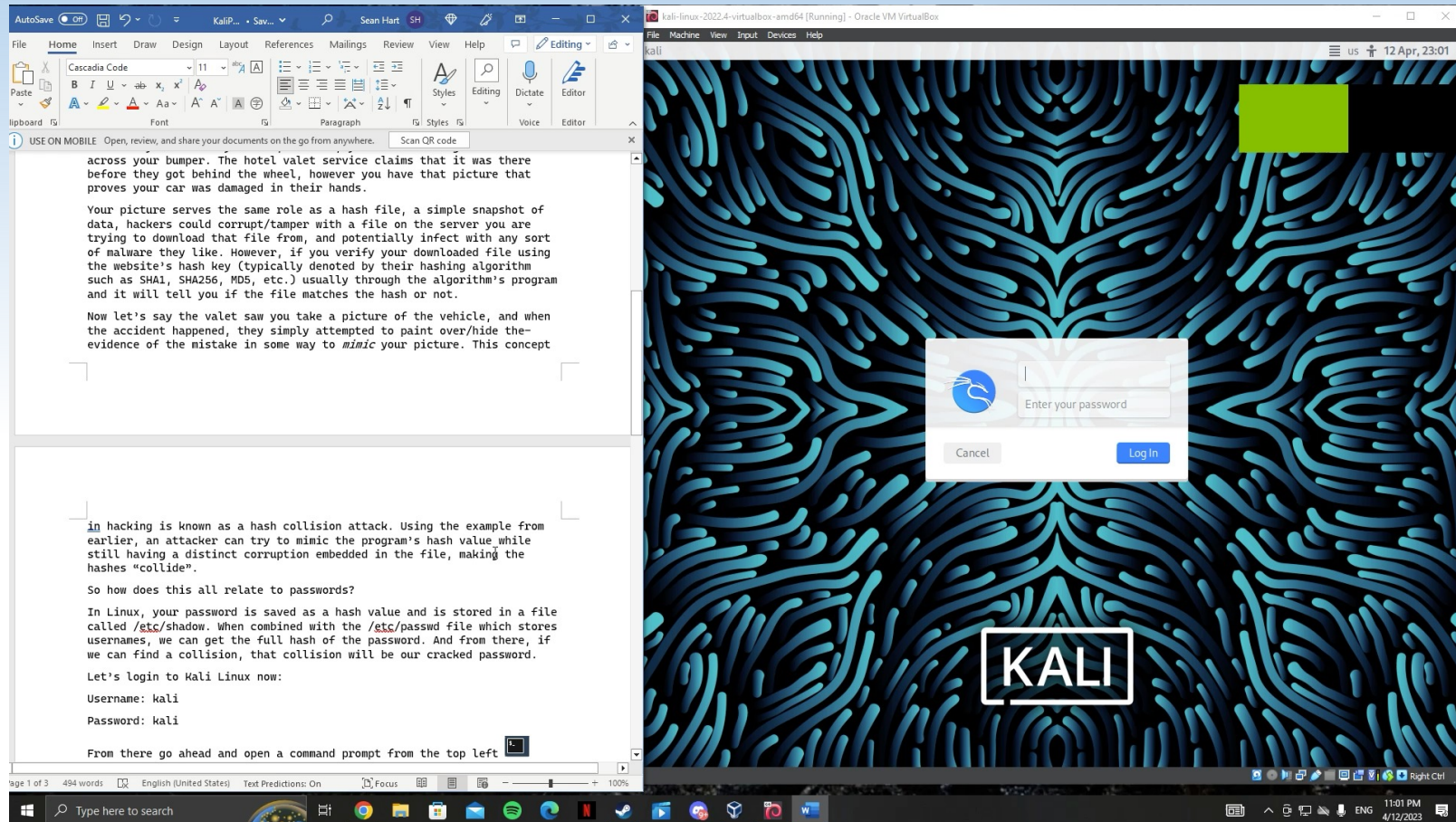
Cons

- Resources
 - File size is very large due to VM sizes
- Dual-monitor implementation
 - Ideal use-case
 - Inconvenient for single-monitor setups
- Trojan executable difficulties

Implementation & Testing

- Software
 - Oracle VM VirtualBox
 - 2-D GUI made with **Unity**
- Tools
 - **Metasploit**
 - Vulnserver
 - ImmunityDebugger
 - Wireshark
 - **SecureEd**
 - Knockd
 - **John the Ripper**
- End-user testing
 - Overall good feedback
 - Dual-monitor setup is ideal
 - Single-monitor setup makes training inconvenient to navigate

Demonstration



Opportunities for extension

- Additional lab exercises
- More engaging features
 - Incorporate videos, mini-games, etc.
- Additional functions
 - Option to print Lab Exercise, zoom functionality, etc.
- Single-Monitor Implementation
- Option to save progress made in training module

Special thanks

We would like to thank the following individuals for their continued support and guidance throughout this project:

- Dillon Tauscher (Co-Advisor)
- Jeffrey Morris (Co-Advisor)
- Jason Orlosky (Professor)

Questions