Lab #1 Learn How to Perform a Replay Attack on Kali Linux Canbus

**Last Name: \_\_\_\_\_\_ First Name:** \_\_\_\_\_\_\_

Objective: Kali Linux is a Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Digital Forensics and Reverse Engineering was chosen as the main operating system of the environment because it provides many applications from password crackers to digital forensics software and is completely customizable. A Controller Area Network is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer. The main aim of this lab is to show the security vulnerabilities of the Canbus. The second aim of this lab is to perform a cyber-attack on the Kali Linux Canbus

Scenarios: A Controller Area Network is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer. Canbus are found in any auto mobiles or other devices. A scenario of this attack would a hacker attack the canbus of automobile in real time or hack a device that consists of Canbus.

Background: Kali Linux is a multiplatform, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains many tools that are fixed on towards different information tasks such as Security Research, Computer Forensics and more. Linux was developed through rewriting of Backtrack by Mati Aharoni and Devon Keams of Offensive Security. Linux contains over six hundred different preinstalled penetration applications that can be discovered. Each program in Kali Linux has its own unique flexibility and case uses. Kali separates these useful utilities into the following categories: Information Gathering, Vulnerability Analysis, Wireless Attacks, Web Applications, Exploitation Tools, Stress Testing, Forensics Tools, Sniffing & Spoofing, Password Attacks, Maintaining Access, Reverse Engineering, Reporting Tools, and Hardware Hacking. Guymager follows under the forensics tools category.

Replay attack is a form of attack where a network communication is intercepted and/or captured and maliciously re-transmitted by an attacker. It is a man-in-the attack in which an attacker sniffs messages being sent on a channel to intercept them and resend them under the cloak of authentic messages. During this attack, the hacker doesn’t need to encrypt the message they resend. However, they can still trick the receiver into thinking the message is authentic. An example of this attack is supposing Alice wants to request Bob to transfer $100 from his account to hers. Alice will send an authentic message to Bob to make this request. Since Bob trusts Alice, he transfers her the amount. Unfortunately, Alice’s initial transfer request was intercepted by an attacker who resends the message to Bob. Bob sees a message he thinks is from Alice, so he again transfers the required amount. However, this time the money is transferred to the attacker instead of Alice.

Goals:

Students will learn these different concepts and terms throughout the various stages of performing this hands-on lab and learning how to perform a virtual cyber-attack (replay attack) on Canbus:

* Learn what kali Linux is
* Learn how to perform a cyberattack (replay attack)
* Learn the vulnerabilities of Kali Linux canbus
* Learn what is Kali Linux canbus

Tools

* Laptops/Desktop
* Kali Linux Canbus

Task

**Skip Task #1 if Kali Linux virtual is installed on your device!**

**Task #1: Installing/Preparing/Starting Kali Linux Virtual Machine**

1. Install the VMware with default options from the website (<https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/15>\_0) if you are using a PC or VMware Fusion or Virtual Box if you are using MAC OS operating system.
2. In a search engine, go to <https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/> website where you will click the Kali Linux VMware 64 bit to get the current version of the computer application. Then unzip the download file.
3. Navigate to the Kali VM that was unzipped and start the virtual machine.
4. Log in to Kali with the username kali and password of Kali.

Task #2: Installing the Dependencies and Downloading and Installing ICSim

1. Type the update command into a new terminal window: **sudo apt-get update**
2. Install the libsdl2-dev and libsd-image-dev with ethe command: **sudo apt-get install libsdl2-dev libsdl2-image-dev**
3. The CAN utilities can be installed using the command: **sudo apt-get install can-utils**
4. Set the directory to the home directory with the command: **cd**
5. The ICSim project files can be download and expand using git with the command: **git clone** [**https://github.com/zombieCraig/ICSim.git**](https://github.com/zombieCraig/ICSim.git)
6. Change into the ICSim folder and list the contents: cd ICSim/, ls

**Task #3: Running the ICSim software**

1. Open three terminal windows
2. In the first window, open the Instrument Cluster Simulator Application(icsim) on the virtual Can network interface created: **~/ICSim/icsim vcan0**
3. In the second terminal window, open the controls app: **~/ICSim/controls vcan0**
4. Right-click (or control-click) on the title bar at the top of the window, and select Always on Top to keep the control panel app visible

**Task #4: Demonstrating a Replay Attack and Replaying the Can Bus Packets**

1. In a separate terminal window, run the can dump tool to log all the traffic on vcan0 to a file: **can dump -l vcan0**
2. Click back on the CANBus Control Panel window and begin pressing keys to accelerate, activate the turn signals, and lock and unlock doors.
3. Click back on the can dump terminal window and press Ctrl-C (control-C) to stop the packet capture.
4. List the contents of the current directory with the ls command, and you’ll see a new file in the format candump-YYYY-MM-DD\_time.log, such as: candump-2019-02-23\_083845.log.
5. Close the CANBus Control Panel window. In the terminal window you were using to run the can dump tool, type the following command: canplayer -I candump-2019-02-23\_083845.log