Lab #2 Learn How to Perform an Injection 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.

Injection attack is type of attack that allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database or change data on a website. During an injection attack, untrusted inputs or unauthorized code are “injected” into a program and interpreted as part of a query or command. The result is an alteration of the program, redirecting it for a nefarious purpose. A real-life example of this attack is in 2014, a hacker gang collected over 1.2 billion unique IDS and password combinations from over 420,000 websites across the internet.

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 (injection attack) on Canbus:

* Learn what kali Linux is
* Learn how to perform a cyberattack (injection 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 and Usage of CarPunk:

1. First type the command: **git clone** [**https://github.com/souravbaghz/Carpunk**](https://github.com/souravbaghz/Carpunk)
2. Second type the command: **cd Carpunk**
3. Third type the command: **sudo bash carpunk.sh**

**Task #3: Use of the CarPunk Script:**

**Type the number of the following command and perform the following actions:**

* [1] Up The CAN Interface : Enable/UP the CAN Interface.
* [2] Down The CAN Interface : Make The CAN Interface Down.
* [3] Start The Basic Sniffing : Start Sniffing Only(get terminal clear as soon as you stop it by ctrl+c).
* [4] Record The CAN Packets : Capture/Record The CAN Packets Into File(as carpunk1.log- name will be carpunk2.log,carpunk3.log,so on for multiple times).
* [5] Play The CAN Packets : Replay The CAN Packets Which You Captured Earlier(specify the log-file. e.g: carpunk1.log).
* [6] CAN Injection DOS Attack : Perform DOS Attack Through CAN Injection.
* [7] ECU Hard Reset : ECU Hard Reset
* [0] Exit : To Exit The CarPunk Script.