Wireless Security (ITSC-301-A)

LAB 2: Password Sniffing

Using Wireshark

Ritika

PASSWORD SNIFFING

Password Sniffing is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public Wi-Fi networks where it is relatively easy to spy on weak or unencrypted traffic.

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection.

Purpose of the lab:

To have you deep understanding of how Man in the Middle Attack and how easy it is to steal sensitive information from the websites which are not secure and also, from the public Wi-Fi. This lab will give you a better understanding of how Active Reconnaissance works.

Tools required: VMware player, Wireshark, KALI and Windows on a VM

Install the ISO image of KALI and Windows on a Virtual machine (VMware). (Take a screenshot of this)

Set up the two VMs in a way they can reach each other (Take a screenshot of this) and then run Wireshark on your KALI machine to capture the traffic between KALI and Windows.

PART 1

On the browser of the KALI box, try logging into an (unsecure) site (http://www.vulnweb.com/) and capture the credentials on Wireshark. (Take a screenshot of this)

Part 2

On the browser of the Windows VM, try logging into an (unsecure) site (http://www.vulnweb.com/) and capture the credentials on Wireshark. (Take a screenshot of this)