Lab 3: Man-in-the-Middle attack with Arpspoof

Introduction
In this lab we will use a Man-in-the-Middle attack (MitM) attack to capture and monitor network traffic. For this lab, we will be attacking a system on your local network (Linux vulnerable machine). The attack will involve using commands like arpspoof, urlsniff and Driftnet. Using these commands, we can view what website a target machine is on and display every graphic that the target is viewing.

Software Requirements
- The VBox Software
- The Kali Linux, as your Penetration Testing Distribution
- Metasploitable2: Vulnerable Linux Platform

Part One: Creating a Man-in-the-Middle attack with Arpspoof
A MitM attack will places our kali Linux system between the router and the target. This way we will be able to see all of the traffic coming from and going to the target system. All traffic from the target system headed to the internet is routed first to our Kali Linux machine, which then captures it and forwards it to the network. All information coming from the internet headed to the target machine is routed through our system first, again so we can view it, and then forwarded it to the target system. We accomplish this by executing the following steps:

- You need to modify the ARP tables on the router and the target system.
- We inform the target machine that our machine is the internet router and inform the router that our machine is the target system
- You need to modify the ARP tables by using the arpspoof program. But first you need to turn on IP forwarding by running the following command:
  ```
  root@kali:~#echo 1>/proc/sys/net/ipv4/ip_forward
  ```
- You need to run the arpspoof command. To do so, you will need to provide the network interface (-i), target system (-t), and the router address.

Arpspoof should then start sending out the modified MAC address.

Part Two: Viewing URL information with Urlsnarf
Let us first look for URL addresses that the target is surfing for by using the following command
Urlsnarf –I eth0

Part Three: Viewing Captured Graphics with Driftnet
Let us view some of the images from visited URLs also. To do so, just use the following command
Driftnet –i
Where (-i) is the interface your listening to.

Part Four:
- Submit a report that describe all of the hacking activities you have been performed. Screen shots be included in the report.

© Happy Spaying!