Project Proposal

Abstract

Sniffing out packet sniffers on a local network, operating on layer two. Exploring methods of identifying packet sniffers who use *Wireshark, Windump*, and *tcpdump* while running promiscuous mode. With promiscuous mode the sniffer chooses to accept all packets, regardless of the destination address. The two methods explored will be ARP spoofing and ICMP forging (With wrong mac address) using either *Hping* or *scapy* for packet forging. This project serves to shine light on identifying passive packet sniffers, while analyzing the development quality of the above packet sniffing tools. The project aims to provide a comprehensive assessment of both the methods of sniffing packet sniffers and the elusiveness of the tools with an emphasis on each side's attempt to unveil or evade from one another.

Presentation Structure

- Introduction
- Exploring how Wireshark sniffs packets
    - Understanding the different settings and filters on Wireshark application: Helps with having a better understanding of what unveiling method might work and might not work.
- Wireshark Sniffing Tool on VM-1
    - Attempt to unveil by ARP spoofing on VM-2
    - Attempt to unveil by ICMP forging on VM-2
    - Analysis of results
- Exploring how TCPdump sniffs packets
    - Exploring TCPdump settings and filters
- TCPdump Sniffing Tool on VM-1
    - Attempt to unveil by ARP spoofing on VM-2
    - Attempt to unveil by ICMP forging on VM-2
    - Analysis of results
- Exploring how Windump sniffs packets
    - Exploring Windump's settings and filters
- Windump Sniffing Tool on VM-1
    - Attempt to unveil by ARP spoofing on VM-2
    - Attempt to unveil by ICMP forging on VM-2
    - Analysis of results
- Detailed assessment of what unveiling methods worked for which tools.
- Detailed assessment of the elusiveness of sniffing tools.