UFMG

Lab - Sniff-then-Spoof

Prof. Ítalo Cunha
Prof. Leonardo B. Oliveira

Agenda

- Goal
- Background
- Machine Setup
- Exercises

Agenda

- Goal
- Background
- Machine Setup
- Exercises

Goal

- Packet sniffing is a common practice of both security experts and attackers
- Spoofing is a common practice of attackers
- This lab gives you an insight on how to work with those techniques

Agenda

- Goal
- Background
- Machine Setup
- Exercises

Protocols

Protocols

- ARP
  - Resolves network-layer addresses into link-layer addresses
  - Mappings are cached
  - An attacker can use spoofed ARP messages to "poison" the cache
- ICMP
  - Used for error information, queries, and other communication properties
  - Gateways can issue ICMP redirect packages to inform hosts of "better" gateways in the network

Tools of the Trade

- Telnet
  - Bi-directional text-oriented protocol
  - `telnet 192.168.51.2`
  - Not encrypted, you can sniff everything
    - Including passwords
- SSH
  - Secure access to remote computers
  - Similar to Telnet, but encrypted

Tools of the trade (Cont.)

- Wireshark and TCPdump
  - Packet sniffing tools
  - Graphic (Wireshark) and command-line based (TCPdump) tools
- Netwag/netwox for attacks
  - Already installed on the virtual machine
  - Netwag is a front-end for netwox
  - Netwox implements more than 200 different tools
  - `Use netwox number --help`
  - We will use only a few of them

Agenda

- Goal
- Background
- Machine Setup
- Exercises

Machine Setup

- General instructions in slides Network - VM Setup
  - Available in our website
- In this lab you might need three VMs
  - Server
  - Client
  - Attacker machine

Agenda

- Goal
- Background
- Machine Setup
- Exercises

General Instructions

- You'll play around with network tools and practice sniffing and network traffic manipulation techniques
- Differences when looking into Telnet and SSH traffic should be observed
- You must set up a malware that spoofs every addressee of PING msgs

Task 1 - Sniffing

- Use Wireshark to sniff ARP traffic on the host-only adapter
- Play around with ARP protocol
- Establish a Telnet session while running Wireshark to better understand the protocol
  - Can you capture a password?
- How much info from an SSH connection you can infer?

Task 2 - Spoofing

- Idea: set up an attack where every ICMP PING msg sent into the network is answered with an PONG msg
    - Even if the target machine is unavailable
- First, make the Client ping the Server
    - Everything will work fine
- Second, make the Client ping an unavailable address
    - The attacker machine must reply that ping with a pong and impersonating the unavailable host

Tips

- Checkout the `arp` command
- Starting Telnet server
  - `$sudo service openbsd-inetd start`
- Starting ssh server
  - `$sudo service ssh start`
- Configure the attacker to spoof ARP and PING msgs
  - Use netwox 73
- If you are running Wireshark with the unprivileged user (i.e., `digitalsec`), make sure it belongs to the `wireshark` group.
  - `$sudo usermod -a -G wireshark digitalsec`

Fill in the form

https://forms.gle/Y84cc3biJf6VjFjT8

Thanks

digital.security@dcc.ufmg.br

Acknowledgment and references:

- This course has been sponsored by the **Intel Strategic Research Alliance program**.
- Security Engineering (Anderson); Computer Networks: A System Approach (Peterson/Davie); Computer Networks (Tanenbaum/Wetherall); Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Schneier, Kohno); The Shellcoder's Handbook: Discovering and Exploiting Security Holes (Anley, Heasman, Lindner, Richarte); Introduction to Computer Security (Goodrich, Tamassia); SEED Project - http://www.cis.syr.edu/~wedu/seed/