Lab 5 - Network attacks

EECS 4481 4.0 Security Lab, Winter 2015

Due: Sunday, Feb 27th, 2015, 11:59pm.

Format: Individual

Learning objective: Familiarization with network protocols (IP, TCP, ARP). Students will use sniffing tools to monitor user sessions on other hosts in the network, and perform active attacks, such as redirecting traffic and issuing a denial of service attack.

1 Passive Attacks

- Using Wireshark, create a CaptureFilter that captures only TCP traffic. Create a DisplayFilter which shows only traffic from telnet. Design a test case scenario that demonstrates the correctness of both filters. Hint: Use any utility that generates non-TCP traffic, such as ping.

  Report: Explain the difference between CaptureFilter and DisplayFilter and provide rules for when to apply one or the other. Describe the test case scenario you used to show the correctness of the two filters you created.

- Use Wireshark to capture all traffic that is sent/received by Linux and Windows workstations during the boot up sequence.

  Report: Analyze the captured traffic and provide answers to the following questions: What are types of network traffic sent/received by both OSs? How would you identify what OS is present from analyzing the capture log?

- Use `nmap` to discover open ports in the three company machines (Windows Server, and the two workstations). Experiment with various parameters for `nmap` in order to discover as much information as possible about the three machines, e.g. the version of the operating system.

  Report: Provide all the information you collected about the three machines including a list of open ports. Provide screenshots that show the `nmap` parameters you used.

- Reverse engineer the `netcat` protocol by executing `netcat` with different parameters, capturing the data, and analyzing the protocol.

Report: Explain the communication patterns of netcat. Include all three phases: connection, termination and data traffic.

2 Active attacks

You must perform the following tasks:

- Assume that you have gained root access to the Linux workstation. Your task is to redirect all http traffic from the Linux workstation to an attacker host for further analyzing of the collected data. Find a way to do this. Hint: Use the `tcpdump` utility for sniffing http traffic.

Report: Include the commands executed on the Linux machine and the commands executed on the attacker host.

- Design a Denial of Service attack using any of the available tools, deploy it, and observe the attack using sniffer tools.

Report: Provide a precise description of your attack.