Activity – TCPDump Basics & Filters

Learning Objectives

- CCNE005 - Identify packet sniffing tools
    - CCNE005.001 - Explain Berkley Packet Filters (BPF)
    - CCNE005.002 - Use BPFs to view multiple protocol types
    - CCNE005.003 - Demonstrate packet decoding features
    - CCNE005.004 - Describe network sniffing
    - CCNE005.005 - Identify common networking sniffing tools

Scenario

- TCPDump is a very useful CLI tool for collecting PCAP information. Its strength is in the fact that it is CLI, and therefore can generally capture much larger amounts of data than Wireshark. The graphic rendering and interpretation that Wireshark performs limits its use for collecting or dissecting very large PCAPs.

Task 1)

- Identify the following basic TCPDump commands/options:
    1. Tcpdump -w capture.pcap
    2. Tcpdump -r capture.pcap
    3. Tcpdump -r capture.pcap port 80 -w http_traffic.pcap
    4. Tcpdump -q -r capture.pcap | wc -l
    5. Tcpdump -i eth0 host 192.168.0.1
    6. Tcpdump -A -r capture.pcap
    7. Tcpdump -c 10 -r capture.pcap
    8. Tcpdump -e -r capture.pcap
    9. Tcpdump -n -r capture.pcap
    10. Tcpdump -S -r capture.pcap
    11. Tcpdump -v (or -vv or -vvv)

Task 2)

- You will need to be familiar with using expressions in TCPDump to capture and analyze traffic on target systems. To ensure you can quickly filter traffic to include the desired transactions/packets, identify the following filters.
    1. Tcpdump host 192.168.1.1 or host 192.168.1.2 && port 80
    2. Tcpdump src host 192.168.1.1 and dst host 192.168.1.2
    3. Tcpdump host www.google.com
    4. Tcpdump src port 80 || src port 443
    5. Tcpdump ether dst host aa:bb:cc:dd:ee:ff
    6. Tcpdump udp port 53 or tcp port 53

7. Tcpdump not port range 1025-65535
8. Tcpdump net 192.168.0.0 /24
9. Tcpdump not net 192.168.0.0 /24

Task 3)

- Now that you have some practice identifying filters, you can practice building filters using expressions.
  1. ARP: Create a TCPDUMP filter that will capture all ARP traffic.
  2. ICMP: Create a TCPDUMP filter that will capture all icmp echo replies coming into interface eth1.
  3. TCP: Create a filter that will capture all the closure packets of TCP conversations (both graceful and not)

Deliverables

- Provide complete responses to the questions above

Hints

- N/A

Challenge

- N/A

Useful Resources

- N/A

Last updated 2018-03-29 15:23:52 UTC