Lab 02 – Analyzing Network Traffic using Packet Capture Software

In this lab, you will capture and analyze network traffic using packet capture software. Every security analyst uses packet capture software to examine and analyze network traffic at some point or another. Sometimes this is accomplished using automated tools and other times this is accomplished using manual methods.

Prior to beginning this lab, you should have a Windows client VM and a Windows server VM configured as a domain controller powered on within your hypervisor environment.

Packet Capturing can be considered an active discovery technique. There is a significant difference between passive and active discovery techniques. Active techniques require prior approval and permission from the target organization. **DO NOT PERFORM active techniques** on a target for which you do not have permission, preferably written within a contract. What does this mean for you? Do not perform active discovery on your organization's network to complete this lab. This lab should be completed in an isolated VM environment, namely, your virtual network security test lab.

Complete the following tasks:

TASK ONE: VM and Wireshark Installation

1. Depending upon how much RAM you have in your host machine, you may choose to accomplish this task using different methods.
    a) The first method would be to create another windows client (or ubuntu linux client – please DO NOT use Kali Linux for this) VM. This additional client would act as your Sniffer which would capture network traffic for the two VMS: your server and your client.
    b) The second method would be to use your host machine as either the Sniffer or the windows client (that is, if you are using Windows).
2. Once you choose which method you wish to use, you will require internet connectivity on the machine you will be using as your "Sniffer". This is where the packet capture software will be installed. You may need to manipulate your hypervisor's virtual NIC on the Windows client VM so you have internet connectivity, if you choose to use this method.
3. Once you have internet connectivity, download the latest version of Wireshark on the Windows client (or linux client).
4. Install this software on your Windows client VM (or linux client).
5. After you have installed Wireshark, reboot your VM.
6. Ensure you have an isolated network where only your Windows server VM, Windows client VM, and your Sniffer are able to communicate with one another. Your Sniffer will be in a passive state, so there is no reason to configure an IP Address on this machine with the exception of this initial connectivity test.
7. Disable Windows Firewall on the Windows server and Windows client VMs.

TASK TWO: Generate and Capture Network Traffic

1. Open Wireshark on your Sniffer VM (or host machine – depending upon where you have this software installed) and begin capturing traffic.

2. Open a CMD prompt with Administrative privileges.
    a) Perform a DNS lookup from the Windows client for the Windows server by name.
    b) Verify connectivity using a ping from the Windows client to the Windows server.
    c) Trace the path a packet takes from the Windows client to the Windows server.
    d) Display the ARP cache on the Windows client and the Windows server. Using ipconfig, verify this information is accurate.
    e) Open a Remote Desktop Connection from the Windows client to the Windows server.
        i. Login to the server using the Administrator credentials.
    f) Using a "net" command, map a network drive from the Windows client to the Windows server's C: drive by using the name in the UNC path mapped to drive Z: on the Windows client. There is no need to create a new share. Use the default one that is already created.
    g) Using other default tools/utilities installed on the Windows client by default, generate two additional types of traffic from the Windows client to the Windows server.

3. Stop the Wireshark capture and save this file as yourfirstname.yourlastname.lab02.pcap.

TASK THREE: Analyze Network Traffic

a) For each type of network traffic initiated in task two provide the following within your report:

- ✓ Screenshots of the tool in use while generating the traffic and the results generated within Wireshark using filters specific to that traffic type. If you cannot accomplish this with a filter, follow the data transmission and provide the details found.
- ✓ What were the results? Describe what's occurring (ie: how does the protocol work…is a request being sent and reply being received?) Document everything as if you were writing this report for a customer.
- ✓ Did you find anything surprising? Or, was everything as you expected?
- ✓ What value will you gain from this tool or source of intelligence? How could this intelligence be leveraged by a bad actor?

DELIVERABLE:

1. Complete a professional write-up and include the following information:

    a. **Description:** Brief description, such as an executive summary, depicting an overall view of what topic or technology you are concentrating on within this lab. Keep this short and to the point. Think like a consultant and be mindful that what you are providing should represent you as a professional in the industry.

    b. **Topology:** Use Microsoft Visio, or Lucid Chart, to create an aesthetically pleasing network topology. This should include devices, network connections, virtual NIC labels, IP Addresses, subnet masks, domain information, credential used, and anything else you feel would be beneficial to add.

    c. **Key Syntax:** Sometimes it's nice to include key syntax used. For instance, if you're not a Linux guru, it might be nice to include how you configured a static IP Address in the Linux CLI, or what files you needed to modify in order to configure a primary DNS server IP Address or domain suffix.

    d. **Verification:** Provide key screenshots that display verification that all tasks and all steps of the lab have been completed. For instance, if the lab required you to login from a windows client to a domain controller, show the screenshot or multiple screenshots verifying this action was achieved successfully. Make sure you provide a description of what the screenshot is showing. Do not simply add the screenshot and state, "here is the screenshot". These descriptions and screenshots should paint a story of the work you put into this lab and verify you have successfully completed the virtual environment configuration. Be thorough and professional! A few things to focus on would be:

        i. Screenshots and tables documenting the intelligence you gathered.

        ii. Think of this report as a professional document that you would be handing to a customer (or provided to management for an organization you work for).

    e. **Conclusion:** Wrap up your lab report with a short conclusion. If something did not work, state it. If everything did work successfully, state that as well.

    f. **References:** Make sure you include any works cited here as well as throughout your lab report. If you looked something up, include it.

2. Upload the following file(s) to the assignment within iLearn:
    a. your .docx or .pdf file of your lab report
    b. your .pcap file

    (please do NOT zip your files)

Good Luck with your lab!