CS 499/ISA 564: Lab 3 – Wireshark and Metasploit

Lab Submission Guidelines

Submissions must be in Microsoft Word or PDF format. Be sure to clearly label what question you're answering. Where possible, screenshots should be embedded directly in the document. Screenshots should be cropped to only include what is necessary to answer the question. If you need to save them as a separate file, save them in compressed format (gif, jpg, png) and name them after the question they pertain to. If your submission contains multiple files, archive them (zip, 7z, tar.gz) and submit the file via Blackboard.

Lab Requirements

- Kali Linux VM
- Metasploitable VM
- Network connectivity between the two VMs

Kali Linux Setup

- Configure VM Networking as Host-Only
- Run *service postgresql start* then *msfdb init*
- Launch Metasploit either by running *msfconsole* within the Terminal or using the Metasploit framework shortcut in the launch bar. Within msfconsole, run *db_status.* It should show "postgresql connected to msf"

Metasploitable Setup

- Download Metasploitable here: https://sourceforge.net/projects/metasploitable/
- If you're using VMWare then just open the VMX file
- If you're using VirtualBox, follow the instructions here: http://hackercool.com/2013/09/how-to-install-metasploitable-in-virtualbox/
- Configure VM Networking as Host-Only
- Ensure that you have network connectivity between the VMs by pinging each of them from the other

Lab 3: Task 1 – Nmap, Ncat, and Wireshark

The purpose of this exercise is to learn how to use nmap for port scanning, ncat/netcat for arbitrary TCP/IP connections, and Wireshark for packet capturing.

Login to your Metasploitable VM and run netcat in listening mode on a port of your choice. You will need to use *sudo*. Make sure your chosen port is not already in use by running *netstat –tnl*.

In Kali, run an nmap scan against your Metasploitable VM. Configure it to scan all TCP ports and to perform OS and service identification and output it to all formats.

Question 1.1 – Provide the normal file containing the nmap scan results (it will have the .nmap extension)

Question 1.2 – Assess the accuracy of nmap's version and OS identification results, what did it get right and wrong? Did it correctly identify netcat? Why or why not? In your own words, explain how nmap does service and OS identification. Hint: Run a port scan against a small list of ports with identified services and leave a Wireshark capture running, and/or read the documentation provided in the Readings folder for Lecture 4.

In Metasploitable, terminate the netcat process and restart it but this time add file execution set to /bin/sh. In Kali, execute Wireshark. It will complain about a Lua error during loading. This error can be ignored. Start a packet capture by going to Capture → Options → Click on eth0 and then Start. Then connect to Metasploitable's netcat process using netcat or ncat. You will not see a shell prompt but you will be able to send commands and receive output. Run some commands of your choosing then terminate the process.

Question 1.3 – Provide a screenshot of the TCP session between Kali and Metasploitable from within Wireshark. Your screenshot should show the commands you executed and the output from them. Hint: Use Right-click → Follow → TCP Stream on the netcat connection to get all the connection data in one shot.

Question 1.4 – In your own words, explain why you're able to see all of this via Wireshark. Imagine if a system administrator was using netcat to perform remote administration functions and that you were in a position to inspect that traffic with Wireshark. What are the potential security consequences in this scenario? (Hint: What if the administrator had to authenticate remotely?) How could that system administrator protect his traffic from eavesdropping?

Lab 3: Task 2 – Advanced Wireshark

The purpose of this exercise is to leverage Wireshark's advanced analysis and workflow techniques to perform basic PCAP analysis and malware hunting.

In the Lab Resources folder you will find 3 PCAP files. Choose one of the files and answer the associated 4 questions for that file. Only answer the questions for the PCAP file that you've chosen and be sure to clearly mark which file you have chosen.

Some helpful tips for these questions:

- The compromised IP address will always be within the RFC1918 ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
- Hostnames can usually be found by looking for the NBNS protocol
- Browsers and operating systems are identified in HTTP User-Agent Strings
- Malware can be identified by Googling for distinctive characteristics such as URL patterns, compromised domains, or suspicious strings in HTTP requests/responses
- For help crafting display filters in Wireshark, read the Wireshark Display Filters Syntax cheat sheet located in the Readings folder

Lab 3-1: Question 1 – Identify the hostname, IP address, OS, and browser of the compromised system.
Lab 3-1: Question 2 – Identify the malware or malicious activity within the PCAP.
Lab 3-1: Question 3 – Provide every IP address and domain name that the infected system checks-in to.
Lab 3-1: Question 4 – Write a display filter to display ONLY the check-in packets. DO NOT use marking or comments to accomplish this.

Lab 3-2: Question 1 – Identify the malware or malicious activity within the PCAP
Lab 3-2: Question 2 – Determine the date and time of the initial malware download
Lab 3-2: Question 3 – Provide every web server IP address that the compromised system connects to
Lab 3-2: Question 4 – What does this malware do to make identification of the web server version and compromised host OS impossible?

Lab 3-3: Question 1 – Identify the malware or malicious activity within the PCAP
Lab 3-3: Question 2 – Provide every DNS query that the malware generates
Lab 3-3: Question 3 – Determine the likely filename of the malware binary
Lab 3-3: Question 4 – One of the compromised system's GET requests for a JPG actually returns data. Is that data a JPG file or not? How do you know?

Extra Credit (10 points) – Choose a different PCAP file and answer the 4 questions associated with it. You will receive 2.5 points for each correctly answered question. Note that you may only do this once.

Lab 3: Task 3 – Metasploit

The purpose of this exercise is to learn how to use Metasploit to perform host discovery, vulnerability assessment, and exploitation.

Use the *auxiliary/scanner/discovery/arp_sweep* module to perform a host discovery across the entire subnet that your Kali and Metasploitable VMs reside in (run *ifconfig eth0* then look at the inet and netmask parameters to determine this). Running this module should add 3 hosts to the host database (confirm by running *hosts*).

Question 3.1 – What is the purpose of performing host discovery (assume you know nothing about the target environment besides the information of your own system)? How does Metasploit's *arp_sweep* module work? How does it know when a host is up? Hint: Use Wireshark to monitor network traffic as the module executes).

Metasploit includes the builtin *db_nmap* command to execute nmap and automatically populate the database with its output. Run *db_nmap* and configure it to scan all TCP ports and to perform OS and service identification on all 3 hosts in the DB. Now that the Metasploit DB contains both host and service information, you can use the *services* command to list all known services for all hosts in the DB.

Question 3.2 – Use Metasploit to exploit the Metasploitable VM. Choose a different exploit from those shown in class. Provide a screenshot showing successful exploitation. Your screenshot must include the name of the exploit used.

Question 3.3 – Write a short (1-2 paragraphs) summary of the exploit you used. What kind of vulnerability did it exploit? How was it leveraged to allow for arbitrary code execution? How could the effect of the vulnerability be mitigated besides by directly patching it? Provide at least one reference link to an online resource that you used to conduct your research.

Extra Credit (10 points) – Metasploit contains many post-exploitation modules that can be used to gather information about a system, maintain persistence, steal credentials, perform reconnaissance, or do various miscellaneous things. Execute one of these modules and explain what benefit this module would have to a penetration tester. Provide a screenshot showing execution of the post-exploitation module.

Lab 3: Task 4 – Armitage

The purpose of this exercise is to learn how to use Armitage to exploit a vulnerable system.

Question 2.1 – Use Armitage to exploit the Metasploitable VM. Choose a different exploit from those shown in class and different from the one you used in Task 3. Provide a screenshot showing successful exploitation. Your screenshot must include the name of the exploit used.

Question 2.2 – Write a short (1-2 paragraphs) summary of the exploit you used. What kind of vulnerability did it exploit? How was it leveraged to allow for arbitrary code execution? How could the effect of the vulnerability be mitigated besides by directly patching it? Provide at least one reference link to an online resource that you used to conduct your research.

Grading

- **Task 1 – 20 points (5 points per question)**
- **Task 2 – 30 points (7.5 points per question)**
- **Task 3 – 30 points (10 points per question)**
- **Task 4 – 20 points (10 points per question)**
- **Extra Credit – 20 points**