Lab 1: Security Tools

Karlstad University

Jonathan Magnusson – jonathan.magnusson@kau.se
Bolaji Gbadamosi – bolaji.gbadamosi@kau.se
Hans Hedbom – hans.hedbom@kau.se

November 20, 2024

1 Introduction

The goal of this lab is to gain first-hand experience on security tools. Security tools are designed for troubleshooting, network discovery, finding vulnerabilities and/or misconfigurations, to test the security of programs and detect bad security decisions. Understanding how security tools work and what they do will help you to better reason about network security and countermeasures.

This lab should be done in groups of two.

2 Preparation

Before starting the lab, it is recommended to get a general idea about the used tools:

- Nmap[3] (important: check the options: -sT, -sA, -sP, -sV and -T) and
- Wireshark [4] (chapters 4, 6 and 7.2 are *very* useful),
- Ettercap [1, 2].

3 Lab Environment

To complete the tasks for this Lab, each group needs:

1. a vulnerable server
2. an attacker machine
3. a client machine
4. a router

For this lab you will get access to a computer in two ways hosting four VMs.

- Access to the computer remotely
- Access to the computer in lab

A simple illustration of the configuration is shown in the Figure 1.

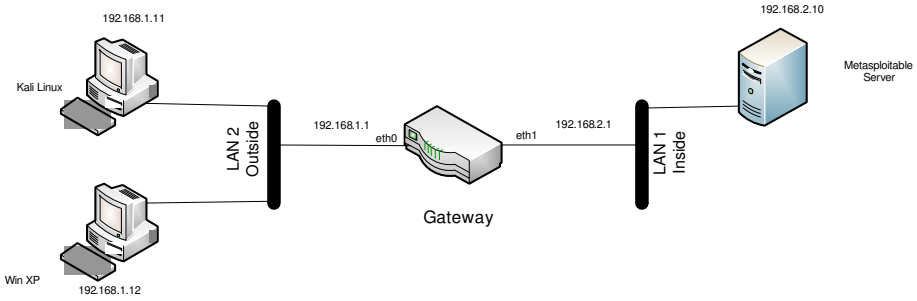

Figure 1: Lab Topology

3.1 To access the computer in lab

1. log in using your student id and password
2. open vmware workstation 15 player
3. in vmware click on: player → file → open.
4. VMs are located in: Windows (C): → vmware → dvgc19-2020

3.2 Access the remote computer

If you are sick you can access the lab remotely

1. go to https://remotelab.kau.se
2. log in using your student id and password
3. open vmware workstation 15 player
4. in vmware click on: player → file → open.
5. VMs are located in: Windows (C): → vmware → dvgc19-2020
6. To exit the computer: windows flag → username (icon) → sign out

The vulnerable server and the attacker machines are running on Ubuntu Linux and Kali Linux respectively. The client machine is running on Windows XP and the router is the Linux machine. Kali Linux provides a rich set of tools to conduct this lab, so no further tools are required.

To access Kali Linux use credentials root/toor
To access Router Linux VM use credentials radmin/radmin
To access the Metasploitable machine use credentials msfadmin/msfadmin

P.S. It is important to start all the VMs (including the router) and login. Click "I copied it" if VMware player asks you. Use Ctrl+g (or click inside the vm with the mouse) to get focus to the VMs and Ctrl+Alt to get focus out of the VMs.

4 Tasks

4.1 Nmap

1. Show the Kali host interfaces and routes (using nmap)
2. Scan the network to find all four devices that are up and running
3. Scan the Metasploitable server for its:
   (a) operating system
   (b) open ports (try TCP SYN/ACK/Connect)
   (c) running services and their versions

You are encouraged to think about: what more can be gathered about your attack surface? What is the lesson you have learnt from this task? Can you think of the countermeasures for some of security weaknesses?

4.2 Wireshark

The goal of this task is to sniff the traffic and get used to Wireshark. Start by launching Wireshark on your Kali VM.

Note: You might need to enlarge your Kali Linux window size to have a better view of Wireshark. To do that go to: Applications → System Tools → Preferences → System Settings → Resolution

4.2.1 Use capture filter to narrow the traffic to http

1. Check eth0 in the interface section
2. Turn off promiscuous mode (if on)
3. Set *capture filter* to tcp port 80

Note: You need to turn off the promiscuous mode in the Wireshark, because it captures not only addressed to the interface traffic, but all traffic that is visible on the interface you are attempting to capture on.

4.2.2 Generate some HTTP traffic

On Kali VM open the web browser and connect to http://192.168.2.10/dvwa/index.php (use credentials admin/password).

4.2.3 Use display filters to analyze the traffic

1. Filter the http request using "http.request"
2. Follow TCP stream: Analyze → Follow TCP Stream
3. Show that you managed to capture the login credentials in the traffic

4.3 Ettercap

The aim of this task to find the username/password of the server. One way to achieve this is to poison the ARP cache of the machines in the network and sniff the traffic for credentials.

1. Turn on port forwarding to enable the Kali Linux to forward the packets it receives. Edit the file: /proc/sys/net/ipv4/ip_forward and change 0 to 1
   - `echo 1 > /proc/sys/net/ipv4/ip_forward`
   - `vim /proc/sys/net/ipv4/ip_forward`
   - `nano /proc/sys/net/ipv4/ip_forward`
2. Open Ettercap and do the following
   (a) Set the network interface to eth0
   (b) Press "Accept" in the top right
   (c) Choose "Hosts" from the menu and "Scan for hosts" from the sub-menu
   (d) Add the router ip 192.168.1.1 as a target 1
   (e) Add the client ip 192.168.1.12 as a target 2
   (f) Choose "ARP poisoning..." from the MITM menu, when prompted choose "Sniff remote connections"
3. Open Wireshark and start to capture on eth0
   Note: Check that you don't have any active filters: Capture → Options
4. From the windows client machine connect to the server (metasploitable machine) on its Telnet port - use credentials msfadmin/msfadmin
   telnet 192.168.2.10
5. Examine the captured packets in the Wireshark for the credentials
   Hint: follow the TCP stream
6. Stop ARP poisoning in Ettercap (top right)

Using Wireshark find out whether you succeeded with ARP poisoning. You are encouraged to understand the motive of this attacker, and to think about other possible malicious motives.

5 Submission

Apart from accomplishing the exercises, we expect you to write a report. The report has to contain the following **four** items:

1. Full names and e-mail addresses of each group member.
2. Describe in two–three sentences each tool (i.e. the different virtual machines and network monitoring tools) used in the experiment and why you need it.
3. Each step of the experiment (what you did and what the result was) should be thoroughly described with your own words.
    - Be sufficiently detailed so that another student could read this and duplicate your experiment. For this purpose, we recommend you to take screenshots and use them in your report.
    - Try to answer the questions, which were stated in the "Nmap" and "Ettercap" tasks.
4. Discuss about the possible mistakes you might have made while conducting the experiments.

Your report should be submitted in PDF format via Canvas. The deadline for this lab (practical part and report) is **December 3, 2024**. Late labs may not be corrected until the next examination period.

References

[1] Ettercap arp poisoning. http://openmaniak.com/ettercap_arp.php, accessed on 2022-10-25

[2] Ettercap (software). https://en.wikipedia.org/wiki/Ettercap_(software), accessed on 2022-10-25

[3] Nmap - network exploration tool and security/port scanner. http://linux.die.net/man/1/nmap, accessed on 2022-10-25

[4] Lamping, U., Sharpe, R., Warnicke, E.: Wireshark User's Guide. https://www.wireshark.org/docs/wsug_html_chunked/index.html, accessed on 2022-10-25