Computer Security | Spring 2015
CS 4351/5352 | Professor L. Longpré

Assignment 4

Introduction:

The purpose of this assignment is to gain experience in network security and network attacks.

General description:

In this assignment, you will use a network simulation tool called core on a Kali-Linux virtual machine. You will first get familiar with command-line tools used in network security and network attacks. You will first use the core program to emulate a network with only 2 computers. You will investigate network routing on a more extensive network. You will then conduct a simple security evaluation on a third network.

This assignment may be done individually, or in a group of 2. You can discuss general concepts about the assignment (e.g., about the setup, etc.) with other groups or individuals, but the answers should be your own. (This will show in your answers, output from tools, etc.) Also, be sure to cite your references. If you do this in a group, each group member will submit the assignment. Each group member must perform the tasks involving the virtual machine on their own computer and submit the required screenshots and output files as generated from their own computer. Parts not involving the virtual machine may be identical for both group members.

In order to avoid facing severe consequences, or simply because you follow proper rules of conduct, please do not use any of the tools or attacks mentioned in this assignment on any network (unless it is yours or if you have written consent!) In particular, if you run some of the tools on the UTEP network, the IT security team will detect your activities and believe you are a malicious user attacking the network. You should set your virtual machine to disconnect from any external network, just in case.

Set-up

You will use the Kali-Linux virtual machine for this assignment. You already used virtual machines so we assume here you already have VMWare or Virtual Box installed on your machine. Here are instructions to get started with the virtual machine.

1. Download the virtual machine (size about 3G) at the following link: `http://www.cs.utep.edu/longpre/kali-linux_403.zip`
2. Extract the virtual machine to a folder (this may take 10-30 minutes)
3. Start the virtual machine either by double-click on `kali-linux_403.vmx` or by starting the virtual machine player (here VMware instructions), open a virtual machine, navigate to where your machine was extracted, select the virtual machine, play virtual machine. If prompted, select "I copied it".
4. The virtual machine should boot. Then, select "other" from the login screen. User name is root, and password is toor.

Part 1: Preliminary questions

1. In this assignment, you will need to enable IP Forwarding. How do you achieve this in Linux (without rebooting), and what is the purpose of enabling IP forwarding. (1-2 sentences)
2. For the following Linux command-line tools, (a) explain briefly what the tool is used for, (b) give an example one line command (including flags), (c) and explain what your example command will do in 1-2 sentences:
   (a) Netcat
   (b) Ping
   (c) Nmap
   (d) Traceroute
   (e) Arpspoof
   (f) Tcpkill
3. For the following applications, (a) explain what the tool is used for in 1 sentence, (b) describe a critical vulnerability associated with the application, and (c) write the port number that the application usually uses for communication:

   (a) Telnet
   (b) FTP

4. What is the Wireshark tool used for? (1-2 sentences)

Below are some references that may be useful to answer (4) - (6):

- Consult the Linux man pages. In Linux, type the command `man <toolname>`
- `http://www.raditha.com/php/ftp/security.php`
- `http://www.slackbook.org/html/basic-network-commands.html`
- `http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/`
- `http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf`

Write your answers to this part of the assignment into a file name part1 (with proper extension, depending on the editor youre using.) Make sure you mention all your sources in this document.

Part 2: Make two emulated network PCs communicate over TCP/IP and collect traffic using Wireshark

Kali-Linux is a security-focused operating system that contains many tools that are useful for security evaluation testing. The provided Kali-Linux virtual machine has the CORE (common open research emulator) software installed. CORE is a network emulator aimed at allowing users to generate network topologies in order to test performance of various communication protocols. For this homework, you will use CORE for network simulations, executing and analyzing impacts of attacks. The simulated networks can include many simulated computers, and the CORE software allows you to open a terminal on each of the computers, in effect having several virtual computers on the virtual machine.

While you perform the tasks in this assignment, again, I suggest you disable the connection to the internet to reduce the risk that your commands interfere with entities outside the virtual machine. Look at the connection icon on the top right of the virtual machine. You can always reconnect if needed.

To start CORE, open a command-line terminal from the menu on the top, and type core. This should open a graphical interface window.

5. Conduct the following steps in CORE

   (a) Using the GUI, create a network with 2 PCs (n1 and n2) and an intermediate device (hub or switch) connecting the 2 PCs.

   Note: when you create the PCs, you will see 2 IP addresses: IPv4 on top and the IPv6 below. For this assignment, ignore the IPv6 address.

   (b) Start the emulation (click the play button)

   (c) Double click on n1 to open a command line terminal

   (d) Double click on n2 to open a command line terminal

   (e) Start Wireshark on n2 (right click n2 and select Wireshark)

   (f) Open your terminal for n2 (from step d.) and use Netcat to start a listener on port 8000. (Make sure to use the listen mode. Type man netcat and see how to run netcat in listen mode.)

   (g) Open your terminal for n1 (from step c.) and use Telnet to connect to the listener on n2 (make sure you use the correct IPv4 address and port) and send your group member names (just type names and hit "enter").

   (h) You should see the traffic with your name(s) in Wireshark. Each line corresponds to a packet. Write the packet number and the timestamp of the packet containing your name(s) in a file called part2.txt

   (i) Stop the Wireshark capture, save the capture as part2.pcapng, and then exit Wireshark.

   (j) Stop the emulation (click the red X button)

   (k) Save your CORE file as `part2.imn`.

Part 3: Investigate routing

Start CORE, click file→open and select `/root/s15_lab4/hw_part3.imn`. Answer the following questions related to the network shown in CORE.

6. What is a subnetwork? (If you dont know, you may search the internet. Mention your sources.) Explain what is the "/24" at the end of the IP address.

7. List all of the subnetworks in the entire network system. How do you know this? (1-2 sentences)

You can get the answers to the following questions using commands mentioned earlier in this document.

8. Roughly how much time does it take before 10.0.1.20 has a route to 10.0.2.10? How do you know this? (1-2 sentences)
9. List the route for traffic from 10.0.1.20 to 10.0.2.10. How do you know this? (1-2 sentences)
10. Which port(s) are open on 10.0.1.20 and 10.0.2.20? How do you know this and what applications are associated with these port(s)? (2-3 sentences)

Write your answers to this part of the assignment into a file named part3 (with proper extension.) Make sure you mention all your sources in this document.

Part 4: Conduct a simple security evaluation

Start CORE, click file→open and select `/root/s15_lab4/hw_part4.imn`. Start the emulation.
IMPORTANT: Assume you only have access to node n4 (10.0.0.21). This means that you should only run commands from n4 command-line terminals and only use Wireshark on n4. You can assume that you know the IP addresses of all connected devices.

11. Take the role of a security evaluator on a penetration test. Your goal is to determine the security posture of the network. You will provide your results to management, and management will give your results to the engineers and/or network architects that can fix the security issues. This means that you must convince management of the severity of the security issues (with evidence) and you must also provide your detailed steps (for reproducibility).

    Write a report that includes your findings, the steps in your process (include tools used and commands executed including IP addresses, etc.). For any security issues you find, you must provide evidence (tool outputs, Wireshark captures and timestamps of packets of interest). Also, briefly mention potential impacts and possible remediation for each finding. Save your report into a a file named part4 (with proper extension.)

Hint. You can check which port is open on each machine in the network, and which application is associated with each port. Some applications send unencrypted passwords over the network. To observe network traffic, you may have to act as man in the middle, by spoofing the ARP table of a machine and using IP forwarding. There may be insecure sessions already in progress in the network. To capture a password, you may have to force the session to restart. Many network protocols automatically restart when the TCP connection is interrupted. You may be able to interrupt a connection from your access point. If you capture a password, you may be able to use it on a machine and collect evidence as to the potential impact of the vulnerability. All of these actions can be done using commands we have referred to earlier in this document.

Part 5: Conclusion

If you have done this assignment individually, you can include this part with your submission. If you have done this assignment in a team, each member needs do this part individually and send it separately from parts 1 to 4.

1. How easy was this assignment? Explain any challenge you encountered and how you overcame the challenge.

2. If you worked in a group of 2, explain your group dynamic, including whether you worked physically together, whether you worked individually and communicated by e-mail, whether you separated the work, and generally, the contribution of each member of the group.

3. Explain what you learned in this assignment.

4. Do you have any suggestion on how to improve this assignment if we use it the next time we teach this course.

Turn in:

You can export files from the virtual machine in several ways. One way is to connect a thumbdrive and connect it to the virtual machine as an external drive. When you disconnect it, it reconnects to your computer. Alternatively, you can use the browser within Kali-Linux, called Iceweasel. From the browser you can e-mail files to yourself. For this to work, you have to restore the connection to the internet, and your computer must also have internet access.
You need to turn in the following, where xxx is an appropriate extension: part1.xxx, part2.pcapng, part2.txt, part2.imn, part3.xxx, part4.xxx.
Turn in by sending an e-mail to longpre@utep.edu. Please use the subject line "CS4351 Assignment 4 submission" or "CS5352 Assignment 4 submission" depending on which course you have registered.

Grading:

Parts 1 to 3: 50%. Part 4: 50%.

Due date:

May 7.

If you turned in your assignment 3 on time with at least half of the parts completed, there is no penalty for the first 7 days after the due date. Otherwise, the penalty for a late homework is 1% per hour up to 10% per day, for up to one week late, counting Saturday and Sunday as well. In either case, submissions may be not be accepted after one week late.

Note: This assignment was derived by modifying a virtual machine setup by Jaime Acosta. The networks provided for the CORE program were also modified from versions created by Jaime Acosta. I want to thank Jaime for his permission.