Network Security

Assignment 3, Wed 6 May 2020, version 1.0

Handing in your answers: Submission via Brightspace (https://brightspace.ru.nl)

Deadline: Wednesday 13 May, 23:59:59 (midnight)

In exercise 3 you will use nmap (http://nmap.org/) to scan the network. I have preinstalled this tool on your Kali VMs. This exercise also requires a new version of the three "netsec-peer" VMs. Download them from https://cs.ru.nl/~dsprenkels/netsec2020/.

Please turn in all your work in plain text files (program source files are also plain text). If you prefer a document with formatting for whatever reason, like including images, use the PDF format to turn in your work (most editors allow you to export to PDF). Note that it's okay to include images separately and then refer to them from within the text files.

1. This question is about IP address spoofing. Write your answers to every subquestion to a file called `exercise1`, making sure to prefix each answer with the letter for that question.

   Take a look at the RFC for the Internet Protocol, RFC 791 (https://www.ietf.org/rfc/rfc791.txt).

   (a) Explain what IP address spoofing is, and what a host on the network must do to spoof its IP address.

   Take a look at the RFC for the User Datagram Protocol, RFC 768 (http://www.ietf.org/rfc/rfc768.txt), and the RFC for the Transmission Control Protocol, RFC 793 (https://www.ietf.org/rfc/rfc793.txt).

   (b) Explain why an attacker cannot just grab any existing IP packet carrying UDP or TCP, change only the IP addresses in there, and expect the target host to accept the packet. Especially for TCP, don't read the entire RFC but focus on the header (pages 15–19).

   During the lecture we explained SYN flooding attacks. Review that now (slide 23 of Monday's lecture ¡https://youtu.be/Xhm-NWz8kVY?t=4298¿). If an attacker wants to do SYN flooding while IP spoofing, she faces a problem. Let's first consider the case where the attacker, Mallory, tries spoofing the IP of an existing host, Bob, to SYN flood her target, Alice.

   (c) Using the TCP RFC, explain which packets get sent to whom when Mallory sends a SYN to Alice using Bob's address as source. Focus on the TCP three-way handshake and the Reset Generation in section 3.4, "Establishing a connection". Explain why this will cause the SYN flood attack to fail.

   When Mallory tries to use the address of Ursula, who's currently not reachable on this network, she does not face the problem you uncovered in the previous question. However, there is now another protocol in play which causes the attack to fail.

   (d) Take a look at the RFC for the Internet Control Message Protocol (https://tools.ietf.org/rfc/rfc792.txt). Read the first five pages, and explain which packets get sent to whom when Mallory sends a SYN to Alice using Ursula's address as source. Explain why this will cause the SYN flood attack to fail.

   (e) Using what you've learned in this course so far, describe a way to make Mallory's SYN flood attack succeed against Alice, while IP spoofing using either Bob's or Ursula's address. You may assume that Mallory is in the same network as Alice. If you make any more assumptions (e.g. Mallory is able to modify all traffic on the network) please state these.

2. This question is about port blocking. Write your answer to a file called `exercise2`.

   As a network security measure, some network administrators attempt to restrict what external services their users can access by blocking any outgoing connection made to all but a few well-known ports. This by itself is not a very effective measure, since it will inconvenience normal users, but it will do nothing to stop somebody in control of the external endpoint.

   Consider you are such a person. You know that soon you will be on a network that blocks every outgoing connection except on port 53 (DNS), 80 (HTTP) and 443 (HTTPS). What could you do to be able to access the SSH service on your external server once you are inside this network?

3. This exercise has you using nmap. Write your answers to separate files in a folder called `exercise3`. So for exercise 3a you should use `exercise3/exercise3a`, etc.

   You will be using the nmap manual page (`man nmap`) a lot, since there will be almost no hints on how to perform the tasks in this exercise. It has a section "examples" near the end. To search the man page, press `/`, then type the string you want to search for, then hit `<Enter>`. To search for the next occurrence, press `n`. To search for the previous occurrence, press `<Shift>+n`. Always use `<Shift>+n` if it seems like the string you are searching for has not been found, since it might occur earlier in the document and by default searching only works forwards. For more controls, look at the `man` viewer manual, using `man less`.

   Note that you will need root rights to execute many of the scan types nmap provides, since they use raw sockets.

   Although all your scanning happens locally, networks are always noisy and unreliable. Especially if you are ever scanning on wireless networks, keep in mind that you are careful in interpreting any scanning results. Try to play with a higher timing template (`-T`), different max-retries or host-timeout, and other stuff, if hosts seem to intermittently drop from the network, or if scans take too long.

   Lastly, we would like you to *think* about your nmap queries. Try to compose commands that are somewhat optimized and only do what you need them to.

   (a) Read the manual page section on host discovery. Your first task is to map the network. Discover all the active hosts, and write your results to `exercise3a`. Also explain how you discovered them.

   In 3a, you could have found at least 5 active IPs on the network. If you did, skip question 3b.

   (b) How can you improve your command from 3a? (Hint: Use `ip address` and look at the netmask, how large is the network?)

   You should have found ≥ 5 "hosts" on the network. However, as you should have concluded in the previous assignment, some of these hosts are backed by the same VM using multiple IP addresses. For the purpose of this exercise, you are allowed to pretend every IP address is linked to a unique host.

   (c) Read the sections on port scanning basics, port scanning techniques, and port specification and scan order. Scan for open TCP ports on the same hosts you scanned in 3a (or 3b). Write your results to `exercise3c`, and explain your scanning techniques.

   If, in 3c, you found open ports on `172.21.153.10`, skip question 3d.

   (d) Why did your command in 3c miss the open port at `172.21.153.10:22222`? Find the other open port on this host.

   (e) Scan for some common UDP ports on the network. You should be able to find one.

   Hint: UDP scans generally take very long. Speed up the scanning process by limiting the amount of ports that are scanned.

   (f) Read the section on service and version detection. Try to detect what services are running on what ports for the same hosts you scanned in 3a (or 3b). List these results in `exercise3f`. Also mention which of these services are running on non-standard ports.

   (g) For all the ports for which nmap is unable to determine what the service is, can you make an educated guess on what kind of service is running there[1]?

   Hint: Search for a list of (unofficially) allocated ports on the internet.
   Hint: Try to talk to the service using standard protocols, and see if they reply.

   (h) *(optional)* If you were an attacker, intent on gaining access to one of these machines, which service would you attack first, and why? Write your answer to `exercise3e`[2].

[1] You likely won't be able to guess correctly for all services, that's okay.
[2] Please don't spend your time on actually attacking this.

4. Place the files and directories `exercise1`, `exercise2`, and `exercise3`, and all their contents in a folder called `netsec-assignment3-STUDENTNUMBER1-STUDENTNUMBER2`. Replace `STUDENTNUMBER1` and `STUDENTNUMBER2` by your respective student numbers, and accommodate for extra / fewer student numbers. Make a `tar.gz` archive of the whole `netsec-assignment3-STUDENTNUMBER1-STUDENTNUMBER2` directory and submit this archive in Brightspace.