Scanning Lab
CSC 9010/5930 - Offensive Security
Grading: 10 points
Due Date: March 20th, 2019 at 11:59 PM

Description: In this lab you will learn about a selection of OSINT gathering techniques and scanning tools. Follow along with the instructions, write your answers to all questions in a separate `answers.txt` file, and submit on Blackboard when finished.

Setup: A number of the scanning tools we will be using in today's lab are very "noisy" and may trigger security measures on Villanova's network. To isolate today's lab environment, you will need to set up a virtual network between two VirtualBox VMs.

1. In VirtualBox, select "Global Tools", then select "Create" to create a new virtual subnet. In the checkbox to the right, make sure "DHCP Server" is enabled.

2. Download the BSides virtual machine from the following link: `https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/`. Once you have downloaded the VM, select "Import Appliance" from the File menu and import the pre-built VM.

3. In the "Settings" menu for both your Kali Linux VM and the imported BSides VM, select "Network" and select "Host-only Adapter" in the drop-down menu. Make sure that the adapter you created previously is selected in the second drop-down box.

4. Boot up both VMs. You can minimize the BSides VM and open the Kali Linux VM for later.

OSINT: Before we start scanning our intended target, we need to understand what targets are available in a given network. For the next portion of the lab, you will be working in your host OS (i.e., not in the Kali Linux VM).

1. The dig tool is a Unix application that allows you to query domain information from DNS about both domain names and IP addresses. Open a web-based version at `https://toolbox.googleapps.com/apps/dig/`. Run several queries over the domain csc.villanova.edu. and answer the following questions:

   (a) What is the name and IP address of the authoritative nameserver for csc.villanova.edu?

   (b) What is the IP address of the web server (i.e., www)?

   (c) What is the IP of the mail server (hint: find the name first by checking the MX record)?

2. Using dig is a helpful way to learn about the specific names and addresses of Internet-facing devices, but we can learn about an organization itself using DNS registrant information accessed through the whois tool. Open a web-based version at `https://whois.icann.org/en` and query villanova.edu, then answer the following questions from the raw WHOIS record.

   (a) How many nameservers does Villanova have?

   (b) What is the administrative email address?

Scanning Tools: After gathering as much information about the IP address space and domain names of a target organization, it is time to start scanning the open devices to see if any exploitable vulnerabilities exist. To do this, you will need to employ a variety of tools depending on the type of devices that are exposed and the types of defenses that are in place around those devices. For the rest of the lab, you will be working in the Kali Linux VM attached only to the virtual network inside your computer.

1. Until now, we have only used our Kali Linux VM as a Linux environment, but it comes with much more. Select the "Show Applications" button on the toolbar to see all of the pre-installed applications, separated by category. The more of these tools you familiarize yourself with, the better you will be able to select the right tool for the job on a real penetration test. For info and documentation on each tool, see `https://tools.kali.org/`.

2. Our first task is to enumerate machines that are online in a given IP address space or on a local network. Open a terminal and use the `ifconfig` command to determine your IP address and the IP address of your local subnet. The subnet address will likely match the first three octets of your IP, followed by ".0/24".

3. Enter the command `arp-scan SUBNETADDR`, substituting in the subnet address for your virtual subnet. This will perform an ARP scan and reveal all the devices connected to your local subnet.

4. If you are not on the target subnet, you can use a ping scan to ping all the devices in an IP address range. Enter the command `nmap -sP SUBNETADDR` to run a ping scan.

   (a) How many devices are connected to the subnet?

   (b) Combining your knowledge from ifconfig and the MAC/IP combinations returned, what is the IP address of the BSides target VM?

5. Having learned the IP address of our target, we can start to gather more specific information, continuing to use nmap. Run a TCP connect scan using `nmap -sT TARGETIP` to port scan common TCP ports for running services.

6. You can add the `-O` flag to the TCP connect scan to attempt to fingerprint the operating system of the target device. Additionally, you can run a version scan with the scan flag set to `-sV` to try to learn version information about each of the running services.

   (a) What TCP services are running? Give the name and port number.

   (b) What OS is running on the target?

   (c) What software and version number is being used to run the web server?

7. There are a variety of different scans and scripting abilities available in nmap, but at this point we know that our target is running a web server, so we will pursue that software as our entry point. If we needed to build a password dictionary or a list of possible network server names, we can run `cewl TARGETIP` to generate such a list by scraping the source files of the web page. Try it now.

8. Unfortunately, there doesn't seem to be that much in the web page, so let's try the server software itself. Use the web vulnerability scanner Nikto to scan for potential vulnerabilities with `nikto -host TARGETIP`.

9. If we want to look for additional files and directories that may not be linked on the web server, the dirb tool will try to retrieve files based on a list of common names (or a list we've generated with cewl). Try running `dirb http://TARGETIP/` to see what additional files may reside on the server.

   (a) Do you see any additional files that look unusual? Name them here.

   (b) Use `curl` to try to retrieve some of these files. Do you see any additional information (e.g., usernames, pathnames, etc.) that could be useful?

   (c) If you find any additional pathnames, can you access the path in your browser? If so, what is produced?

10. Our continued efforts have uncovered a running Wordpress blog on the server. Since Wordpress is a widely used application that is open source, there are tools that exist specifically to exploit it. The last phase of our intelligence gathering will focus on searching for Wordpress vulnerabilities specifically.

11. Using the tool wpscan, try scanning for vulnerabilities. Enter `wpscan --url http://TARGETIP/WORDPRESS_URL`.

12. Success! There are a variety of different vulnerabilities in this particular version. Next, let's enumerate the users by adding the flag `--enumerate u` to the previous command.

13. Finally, we can try to brute-force the passwords of these users with lists of common dictionary terms. Add the flag `-w PATH_TO_WORDLIST` to brute force the passwords on the server. You will need the path to a specific word list to do this. Fortunately, Kali comes with several pre-installed. It will take some time, but try `/usr/share/wordlists/nmap.lst` as your input word list (while the scan runs, you may want to skip to the "Explore Kali" part of the lab and do some reading).

    (a) How many vulnerabilities did wpscan find?

    (b) What theme is being used? Are there any plugins installed?

    (c) What usernames are on the system?

    (d) Were you able to recover or deduce any passwords based on the output of the brute force scan? If so, try it out in a web browser and see if you can log into the system.

14. At this point, you have a significant amount of information about the services and users on this particular machine. In next week's lab, we will look at tools that will help us exploit the findings from all of this vulnerability scanning.

Explore Kali:

1. For the remainder of the lab, select a new scanning tool from the list of Kali Linux tools (`https://tools.kali.org/`) and answer the following questions:

   (a) What is the name of your selected tool and what is its intended scanning purpose?

   (b) What additional information does your tool yield about the BSides VM?

   (c) How helpful did you find today's lab exercise? What helped your learning the most? What would you change?

Rubric:
(10 points) submit your answer sheet on Blackboard.

Deliverables: Submit the answer sheet on Blackboard.