Lab #6

Class: CECS 303 – Networks and Network Security
Instructor: Chris Samayoa
Due Date: April 13, 2022 by 9pm PST

Objective: There are two tools that you will be exploring in this week's lab: strace and Nmap.

'strace' is a diagnostic tool for Linux distributions that allows an administrator to monitor system calls and changes in process states. Using strace, this lab will walk you through intercepting a set of SSH credentials while logged into the SSH server. This is an example of an attack that can occur on a machine that has already been compromised and the attacker has root access.

As discussed previously in class, Nmap is a scanning utility that can be used as a valuable reconnaissance tool to learn information about potential targets. Nmap will be used to scan a hosted URL (ad.samsclass.info) and conduct a "capture the flag (CTF)" style exercise.

Sam Bowne is an instructor at City College San Francisco and maintains a website to help teach various computer networking and security courses. As part of this website, he hosts labs that either need to be configured using virtual machines or are hosted by him.

Legend:

- *Server*: refers to the two Ubuntu Server VMs that were created in Lab 1
    - *Apache Server*: refers to the server VM with Apache installed on it
- *Workstation*: refers to the Ubuntu Desktop VM that was created in Lab 2

Links

- strace Basics: https://linuxhint.com/use-strace-linux/
- strace Exercise: https://samsclass.info/123/proj14/H131.htm
- Nmap Exercise: https://bowneconsultingcontent.com/pub/EH/proj/H410.htm

strace Exercise

Navigate to the exercise for strace listed in the 'Links' section above (H 131: Stealing an SSH Password with strace). For this exercise you will be using your two Ubuntu server VMs. On one server VM (**server 1**) you will create a test user "waldo", install strace, and launch a second SSH process running on port 2222. On the other server VM (**server 2**) you will initiate an SSH session to server 1 which will have its credentials intercepted. I recommend using Putty to SSH into your two server VMs for easier use.

The goal is to complete 'Flag H 131.1: Stolen Password' successfully.

1. Note, you will need the proper iptables rules in place to allow SSH connections (TCP port 22) inbound and outbound from both servers or this exercise will not work. These rules should already be in place from previous labs, but verify that they are there using the 'iptables –L' command.
    a. If your iptables need to be adjusted, review Lab 3 for instructions on how to allow traffic inbound (INPUT chain) and outbound (OUTPUT) from your servers.
2. Skip the section on "Adjusting the Google Cloud Firewall"
3. Begin from the section titled "Creating a Test User" and follow the instructions
    a. In the first part of this section for creating the test user (named waldo), ***use the following for your password: cecs[your initials]***
4. Complete the remainder of the instructions on the page
    a. The following sections are completed on server 1:
        i. Creating a Test User
        ii. Installing strace
        iii. Launching a Second SSH Server
            1. The instructions here state to use 'nano' to modify the sshd_config file that you copied to your root folder – feel free to use 'nano' or 'vi' to edit the file
            2. Ensure that you are editing the copied ssh_config file NOT the original during this part
        iv. Finding the Correct Process
        v. Flag H 131.1: Stolen Password

1. After verifying that you successfully stole the password, *take a screenshot of the output from the command 'head foo' for your deliverable*
2. Password shown should be as specified above in step 3a: 'cecs[your initials]'

a.
```
cnit_123a@deb10a:~$ head foo
strace: Process 23927 [redacted]
restart_syscall(<... resuming interrupted poll ...>) = 1
read(6, "\0\0\0\v", 4)                  = 4
read(6, "\f\0\0\0\6sekret", 11)         = 11
getuid()                                = 0
openat(AT_FDCWD, "/etc/login.defs", O_RDONLY) = 4
fstat(4, {st_mode=S_IFREG|0644, st_size=10477, ...}) = 0
read(4, "#\n# /etc/login.defs - Configurat"..., 4096) = 4096
read(4, " issuing \n# the \"mesg y\" command"..., 4096) = 4096
read(4, "t supports passwords of unlimite"..., 4096) = 2285
cnit_123a@deb10a:~$
```

b. The following sections are completed on server 2:
    i. Logging In
    ii. Entering Password

Nmap Exercise

Navigate to the exercise for Nmap listed in the 'Links' section above (H 410: Nmap). This exercise can be run directly from your laptop (no VMs needed).

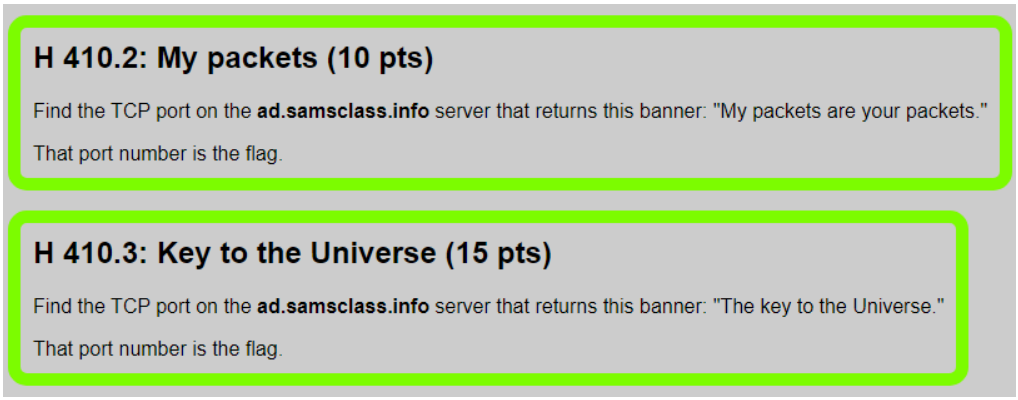
The goal is to complete 'Flag H 410.2: My packets' and 'H 410.3: Key to the Universe' successfully.

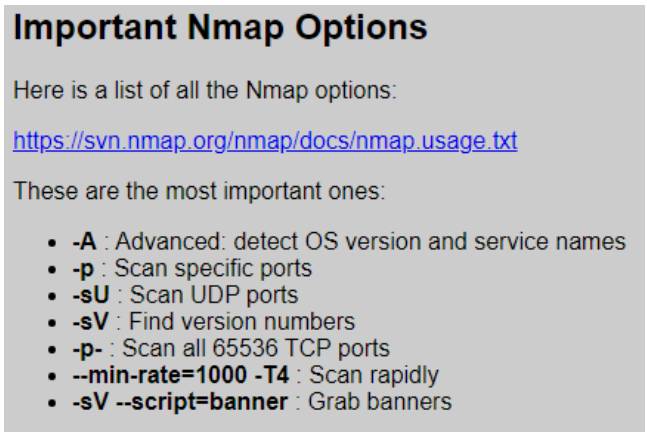
1. Install Nmap
    a. Windows / Mac: https://nmap.org/download
    b. Linux
        i. 'sudo apt update'
        ii. 'sudo apt install nmap –y'
2. After installation is complete, run a test using localhost
    a. Open a command prompt on your machine
        i. 'nmap localhost' will run a regular scan for open ports

ii.
```
C:\>nmap localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-06 22:27 Pacific Daylight Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00052s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
843/tcp  open  unknown
2869/tcp open  icslap
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

C:\>
```

3. Read through the sections of the exercise listed on the 'H 410: Nmap' webpage, but you will be skipping most of the specific instructions.
4. Complete H 410.2 and H 410.3 listed at the bottom of the page
   a. 

   b. Hint: Pay attention to the 'Important Nmap Options' section of the lab webpage
      i. 

   c. Optional: You can verify your answers on this page before submitting to BeachBoard: https://bowneconsultingcontent.com/pub/CTF-A2020/index2.php?type=H

Deliverables (submit via BeachBoard)

1. Compile the screenshot requested for Flag H131.1 in a .doc, .docx, or .pdf file along with the TCP port numbers that were the answers for H410.2 and H410.3.