First of all, I downloaded the given .ova file. I tried to run it on my VMWare, but there was error pop up. I downloaded the given .ova file again, but same happened. Then, I downloaded Virtual box and started given file in it.

I had Kali machine in VMWare, I exported it to VirtualBox and then run it.

I run the following commands on my kali root terminal.

Cmd :- Ifconfig :: This command gave me my kali machine’s IP, The more important thing I got was netmask. If I try to scan nmap, then many students can be connected through institute ID. My netmask was 255.255.255.0 can be represented as 11111111

11111111 11111111 00000000, in short /24 type.

Cmd :- nmap <kali ip>/24 :: This command will scan all the available IP’s of my type, which means the last eight bit of IP is different from mine and as expected there appeared three hosts, my desktop, my kali and my .ova machine, my kali machine had 0 ports available and another IP had .microsoft service running on one of its port (i.e., that was my desktop) and the remaining IP was for vuln.ova.

Cmd :- nmap -A <target-IP> :: This command performs aggrasive scan, In which I identified that .ova machine was running on 9.10.3-P4-Debian version and in detail I found out that only one port 53 was running on TCP service. So, basically I have now version of linux system of vulnerable device.

Then I entered vuln.ova and logged in as guest. I wrote command and found out that currently 3 local servers are running, on one of them I found out something strange written looking like I should know sql but I haven’t learn sql yet, so I proceeded forward.

I tried to access file that stores password. (/etc/passwd ), I accessed it columnwise, I tried different passwords from that and tried to login for root user, saic user, checked permissions for different user folder, tried sudo, but any of that didn’t work.

Then I again started checking all the systemfiles, in one file I found seed.sql and another with them, where I found email id and encrypted password, I tried password decripograph by 8bit ->6bit -> hexadecimal conversion (this method has a particular name, I don’t remember it as I was watching that vedio just for fun), but it didn’t work and I don’t know other type of encryption solve and so I left it.

Now I don’t know what to do next, so I tried out youtube, chatgpt and prompted nearly 2 hours, tried different ways, but most of them used Metasploit.