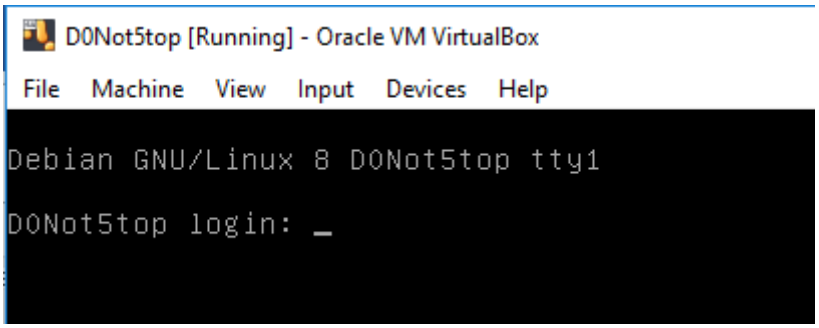
CYBERSECURITY

SCANNING AND ENUMERATION: D0NT5STOP

INSTALL TARGET

Download the D0NT5STOP image from Canvas. (Or find it on the vulnhub website.)
The image comes in the .ova format so we can simply import it into Virtualbox.
Make sure that the image is connected to your "host-only" network and that this is the ONLY interface present.
After startup, it should show:



SCAN

IPDISCOVER

We don't know the target's IP address and can't logon, so let's perform some scans.
Besides nmap, another scanning tool is netdiscover. Check it's options…
From KALI's console we do a "netdiscover r a.b.c.d" with a.b.c.d = range created for your local network.
Document your findings.

Within VirtualBox, we check the MAC-address for network adapter on the Target machine. This way we can link the IP address to the MAC address. (If you only have one address returned. You know that this is the one.)

So you know that the IP address is:…….

You can test if you can ping it. (Isn't blocked by machine.)

NMAP

Let's do a simple nmap to it's IP to see which services are present.

Also do a nmap -sV to see if there's extra target info. What is the advantage of this?
Try a nmap -sV -vv to get extra scan-info.
And finally try a nmap -sV -O. Does it work?

Extra question: how can you prevent nmap from pinging/discovering hosts?

ENUMERATE

We saw that the target machine has port 80 open.
Using your KALI-browser, try to connect to the machine.
What do you get?

ENUM1

Try a first enumeration by using the “nikto” tool: nikto -h targetIP
More information here: https://tools.kali.org/information-gathering/nikto
It will enumerate web-server vulnerabilities.

Document your findings.

Questions to check:

What information do you learn/see?
What would be usefull to exploit later?
Help: pay special attention for the installation of wordpress (wp-admin) and the /php/admin directory.

ENUM2

Lets try the “dirb” tool: dirb http://IPtarget
More information: https://tools.kali.org/web-applications/dirb
Through its “wordlist” it will try to find standard paths of installed webapplications.
Where is the wordlist located?
Drib will enumerate usefull paths.

Document your findings.

Conclusion:
We are now ready to perform exploitation of this machine.