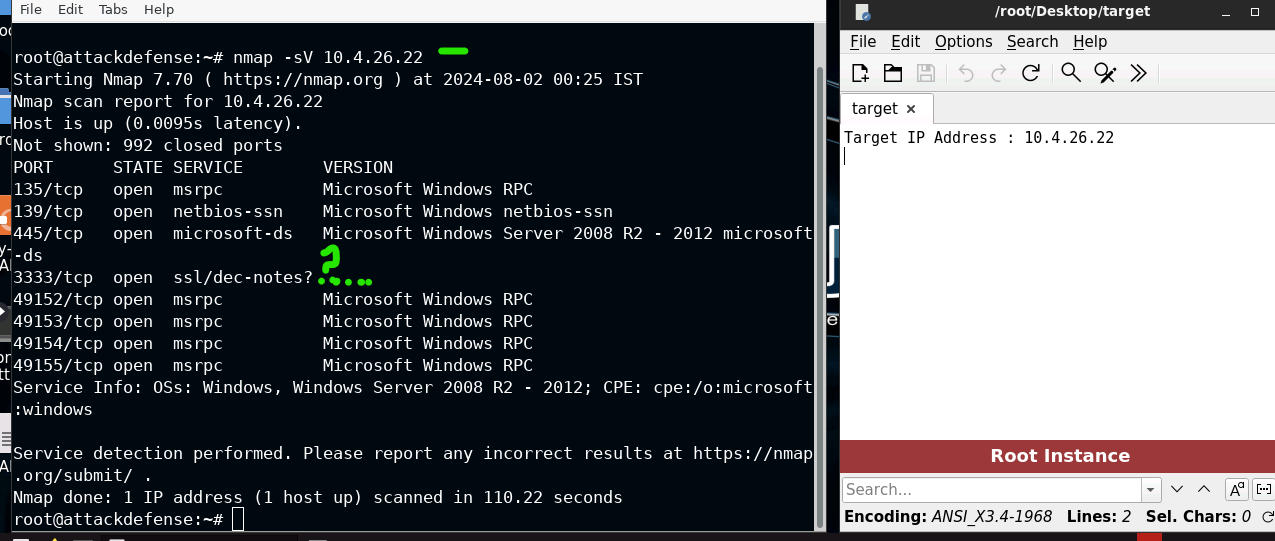
RDP exploitation: (Yay! We actually get to use hydra for once! )

RDP allows GUI remote access for Microsoft systems; lets you click on a remote machine’s screen.

Typically, this is on TCP 3389, but can be configured to other ports too.

Objective: brute force credentials to RDP and authenticate into the target machine.

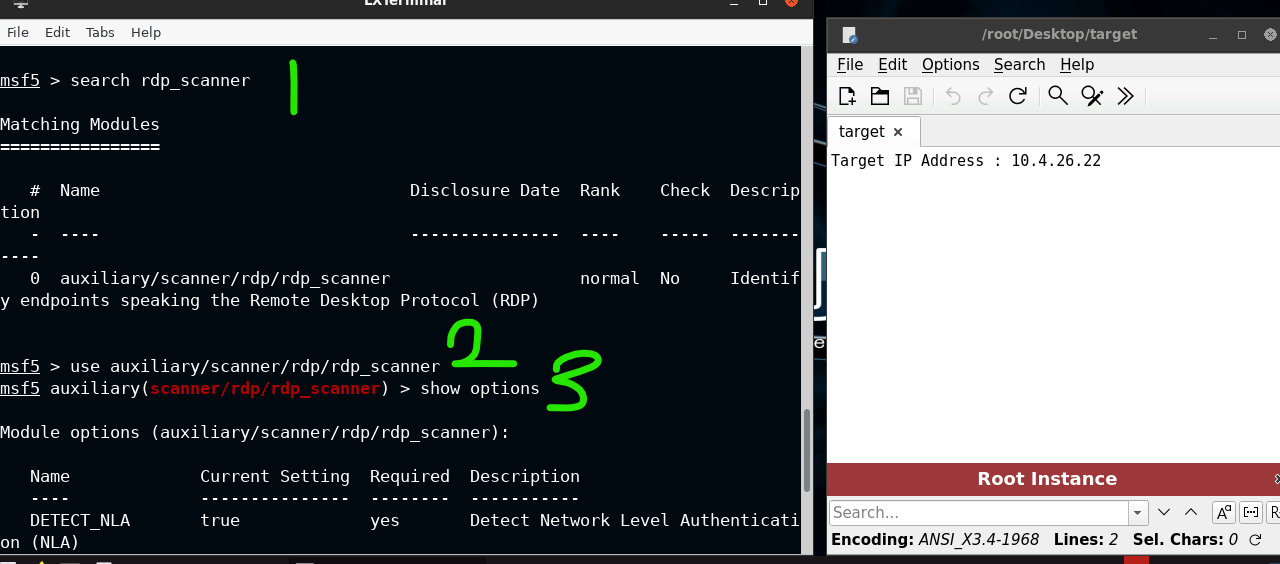
Nmap shows we got port 3333 open, which is a bit of a funny one.



(Screencap shows we got some activity on 3333. )

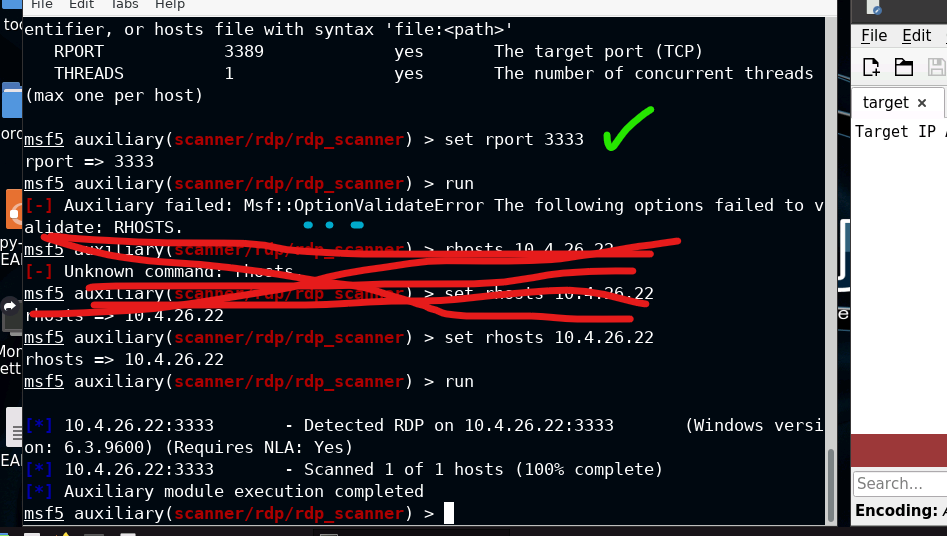
We don’t know for sure if RDP is running on here, so we need a scanner to confirm that it is, indeed, an RDP service over 3333

Search for an rdp scanner, then check the options, since we need to point it to the right port.



It’s RPORT that we need to change.

Also, don’t be an idiot, and actually set a target at the rhosts ip address.



After that lapse of stupidity, we see the scanner gives us a notice that it Detecterd RDP on 10.4.26.22:3333.

That’s our target, and the port we were interested in, so we’re in business. (this output implies a larger scan could be done on multiple targets, but this is out of the scope for this lab. Sucks that the teachers don’t expand on details like this though)

Next, using Hydra for an RDP brute force…

From command line, using hydra as a brute-forcer:

Command:

hydra -L /usr/share/metasploit-framework/data/wordlists/common\_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt rdp://10.4.26.22 -s 3333

English:

Use hydra with the login selected from the possibilities in the common\_users.txt file.

Select passwords from unix\_passwords.txt.

The target is at ip address 10.4.26.22, and we’re connecting over RDP (remote desktop protocol).

We need to use -s to switch the port from the default (usually 3389 as a standard) to the identified 3333 we found while doing recon.

From the official program itself:

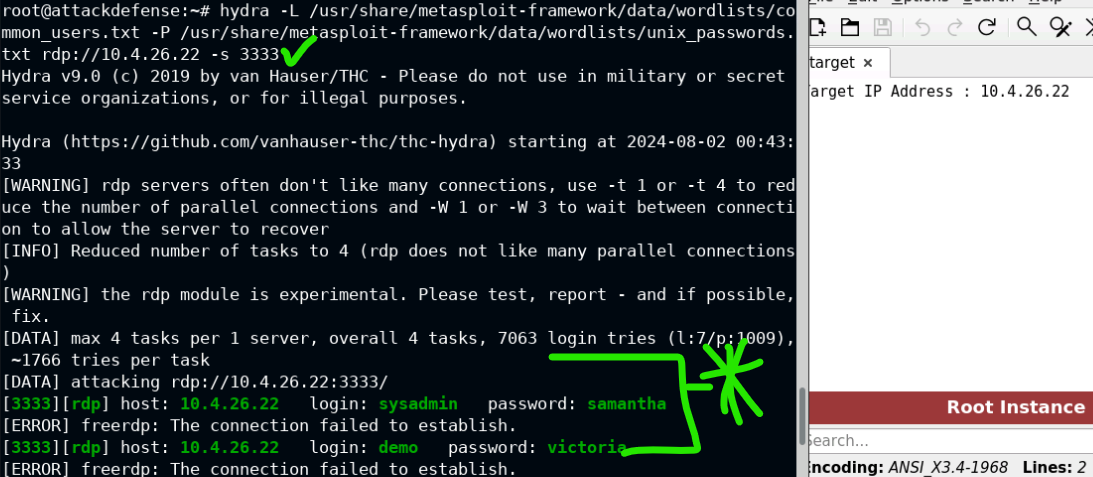
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover

Note: the above command is extremely aggressive and has no wait times implemented.

See below, adding these flags with -t 1 (only a single task at a time rather than the default 16 hydra uses).

Also, waiting 2 seconds between attempts.

hydra -L /usr/share/metasploit-framework/data/wordlists/common\_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt rdp://10.4.26.22 -s 3333 -t 1 -W 2



…

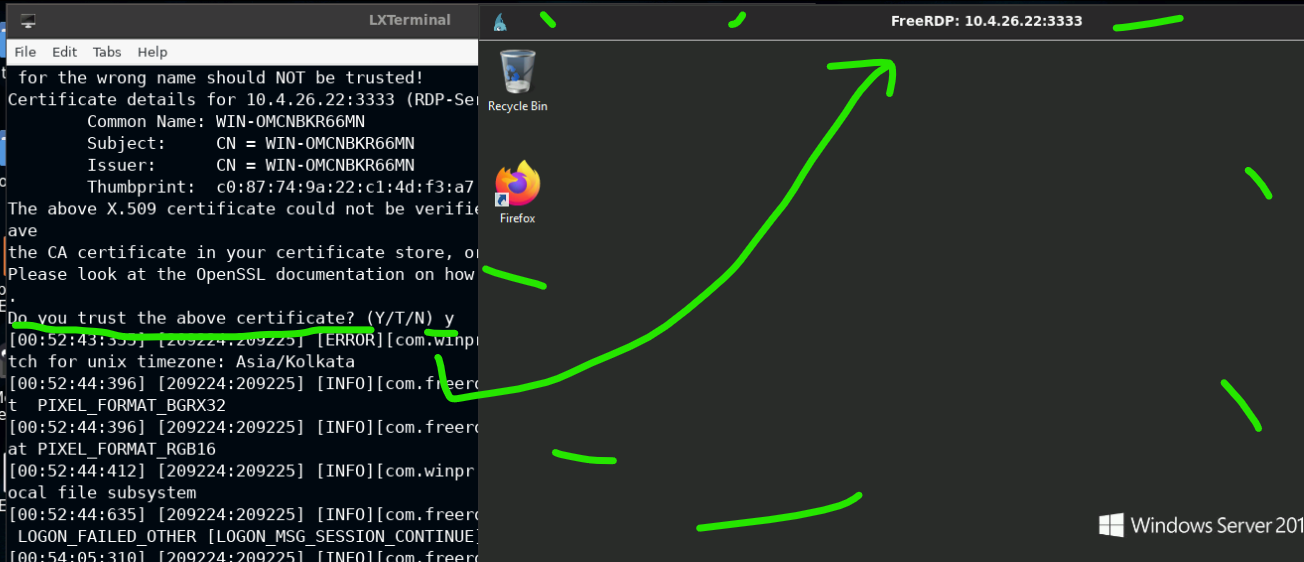
With credentials found, we can access RDP through using xfreerdp as a thing.

(in typical fashion, this is just pulled out of thin air and you have to know it exists and fits the bill for this scenario)

Note that we specify our target with /v:ip.add.re.ss:port

So after the IP we do the port that was different than the default, here being 3333

Command: xfreerdp /u:administrator /p:qwertyuiop /v:10.4.26.22:3333



And there you go, we got our remote desktop access.

Now if only the practice labs didn’t have weird window-resizing to make this environment completely useless as a GUI…