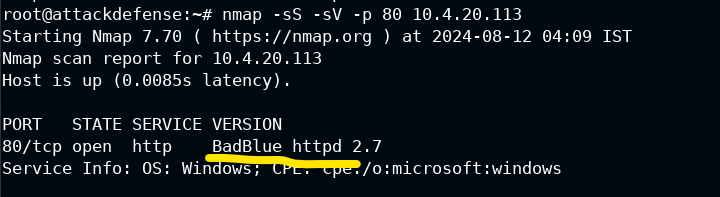
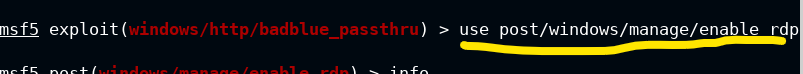
Start with a -sV scan from nmap. We got bad blue running on the target.



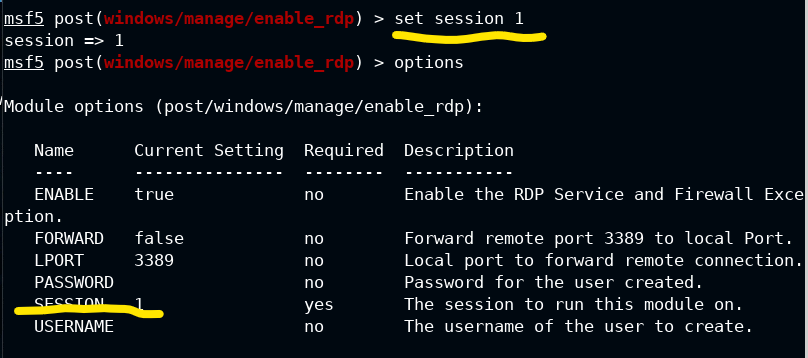
Use the matching exploit, baddblue-passthru



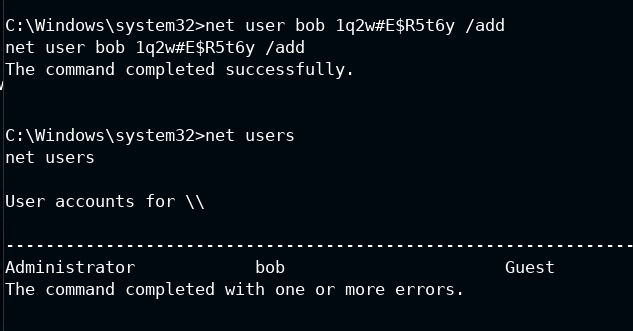
To be cool, we’re activating rdp



This exploit just needs us to set the session, which we can check under options



If we want to pivot, we can set up a new user, shown as adding bob here

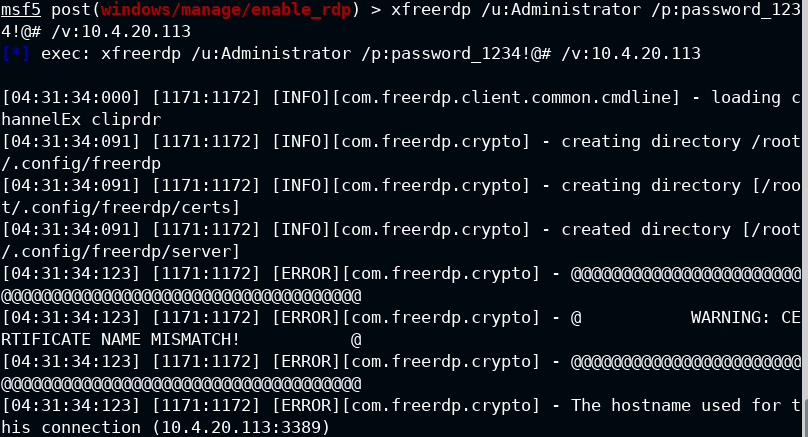


However, we also have the admin, which we can change with command

Net user Administrator passweor\_123

The above command changes the password of administrator to the indicated one

We can then use these credentials to log in



There is a flag on the rdp desktop of the target

