**Lab - Performing an RDP Brute Force Attack**

**Overview**

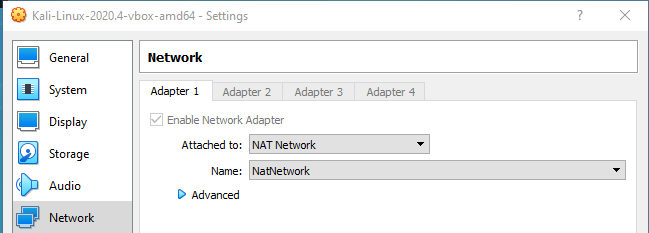
In this lesson, you will learn how to exploit RDP running on a remote target using brute force attack. The current global pandemic has forced many office workers to work from home and remote into their networks using Remote Desktop Protocol or RDP. System administrators rely on RDP to perform administrative tasks on servers and workstations remotely. This sudden surge in remote access has also seen a significant spike in the number of RDP-related attacks.

Gaining RDP access gives the attacker complete control over the target machine.

**Lab Requirements and Preparation**

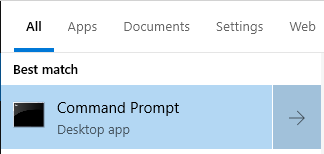
* One virtual install of Kali Linux.
* One virtual install of a Windows Operating system, either Win7, Win10, Server 2012, 2016, or 2019.

Ensure your VirtualBox network settings for both machines are set to NAT network.

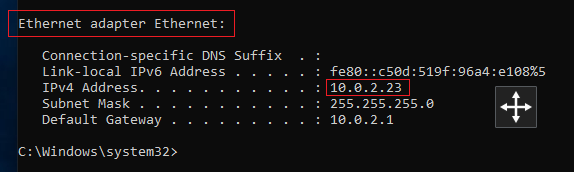


**Configure your Windows Target for RDP**

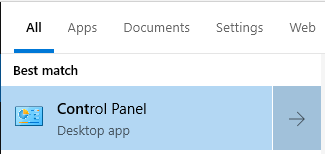
From your Windows search, type cmd. From the results, click on Command Prompt.



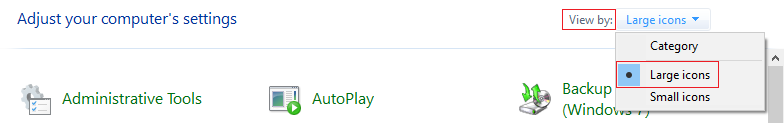
At the prompt, type ipconfig. Find the IP address assigned to your target machine. Take note of the IP address, or leave the command prompt up to display the information.



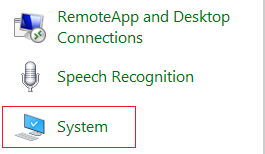
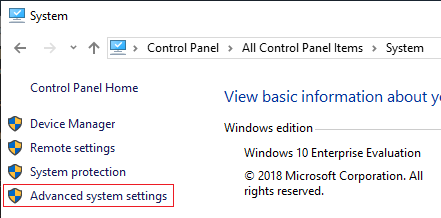
Back at the start menu and your search bar, type control panel. X2 click to launch.



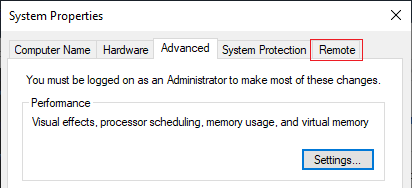
On the Control Panel page, change the view type to large icons.



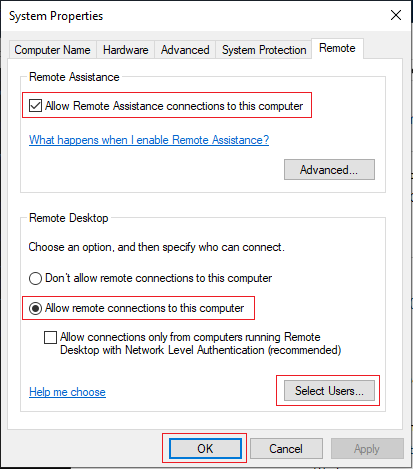
On the next page, scroll down until you find System. X2 click to launch. On the System screen, from the menu on the left, open Advanced System Settings.



Click on the Remote tab.



On the next page, configure your RDP settings as shown in the following image. Click the Select Users button. I added the local user account to the Remote Desktop Users group. I recommend you do the same.



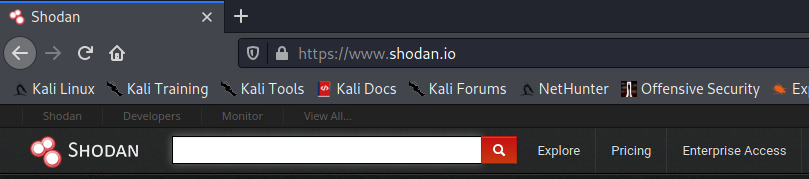
Click OK, close out all windows, and return to your Windows desktop. Minimize your Windows target and open your Kali Desktop.

**Find an RDP Target Using Shodan**

For this lab, we are using a very sterile environment. We have two virtual machines running on the same network configured to see each other. What if your target was on the Internet and you needed to confirm that the target was vulnerable to an RDP brute force attack?

We could the Shodan search engine, and using the outside IP address of the server, we could search to see if RDP was running on the remote machine.

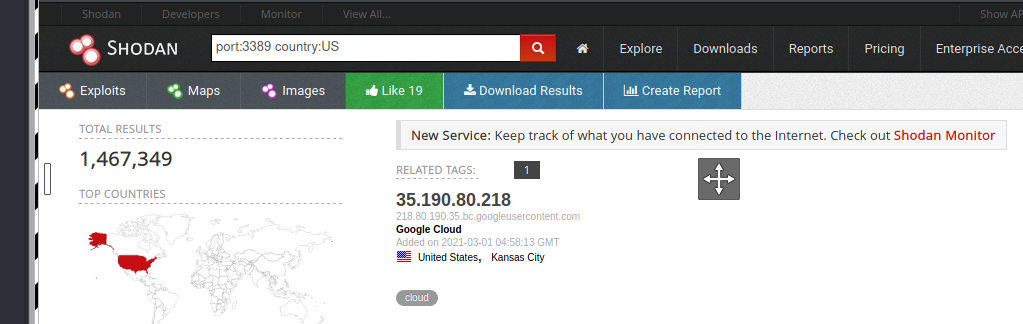
From your Kali machine, launch a browser. In the address bar type, shodan.io.



To use search filters, you will need an account, and you will need to be logged on.

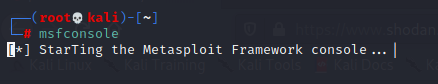
In the search bar, you could type the IP address of your server that faces the Internet and check to see what protocols are running.

What if I don’t have the target IP address, and I’m just looking for a target in the U.S.? I could search for, **port:3389 country:US**



We have located a target. I need to scan the target to ensure it is vulnerable to an RDP brute force attack. For this, we can use an auxiliary scanner found in Metasploit.

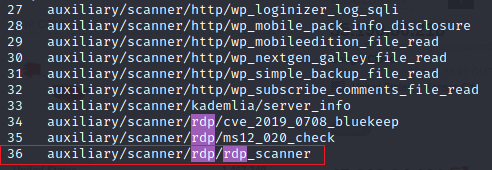
From your Kali machine, open a terminal. At the prompt type, **msfconsole**.



Once Metasploit has started, we can search from an auxiliary RDP scanner using the Metasploit search feature. At the msf prompt type, **search rdp**.

From the search results, under auxiliary, find number 36,

**auxiliary/scanner/rdp/rdp\_scanner**

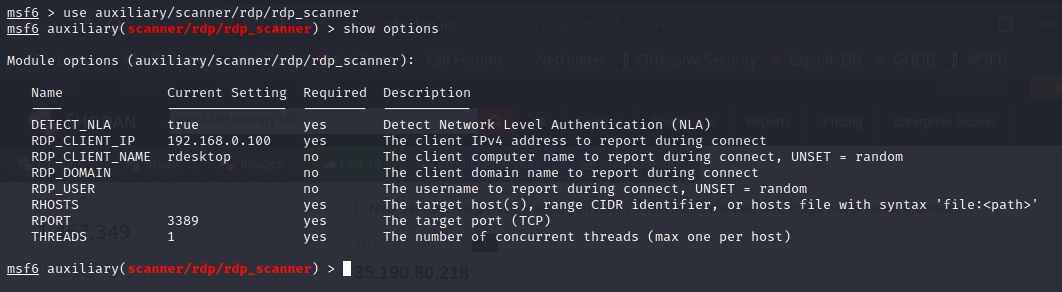


Highlight and copy the name of the scanner. 

At the msf prompt, type the word **use** followed by the name of the scanner you just copied.



This loads the selected Metasploit module. At the prompt, type **show option**s. Press enter.

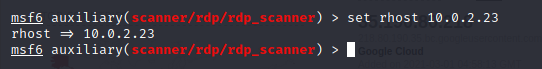


The only option we need to concern ourselves with is setting the IP address for the remote host (RHOST).

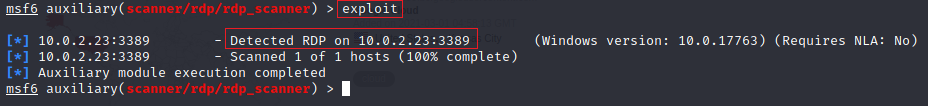
Since I do not have permission to scan any target on the Internet for RDP, I will be scanning my Windows 10 target.

At the prompt, type **set rhost** followed by the **IP address of your remote target**. Press enter.

**set rhost 10.0.2.13**



At the prompt, type in the word, **exploit** to launch the scan.

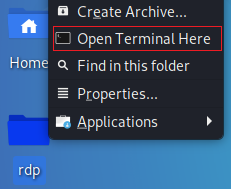


Notice the results come back, letting us know the remote target is running RDP.

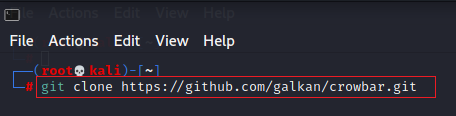
**Launch the attack**

For this attack, we will need to download the hacking tool, Crowbar, from Gitlab.

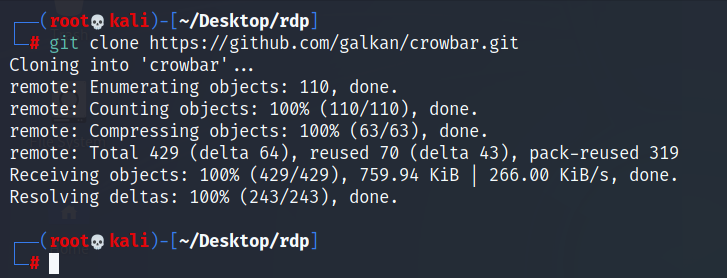
Minimize your open windows and from your Kali Desktop, right-click on your rdp working folder and from the context menu, and select an **Open Terminal Here**.



At the terminal prompt, type git clone and paste the URL you copied from the Gitlab site.

**git clone https://github.com/galkan/crowbar.git **

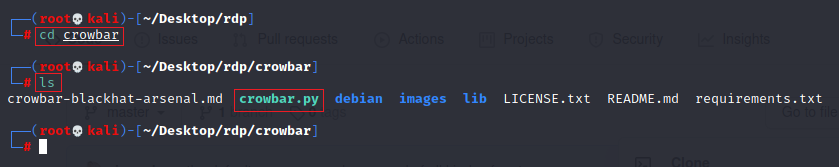
Press enter. The crowbar package is copied and saved to your working folder.



Let’s look at crowbar. At the prompt, change the directory location to the crowbar directory.

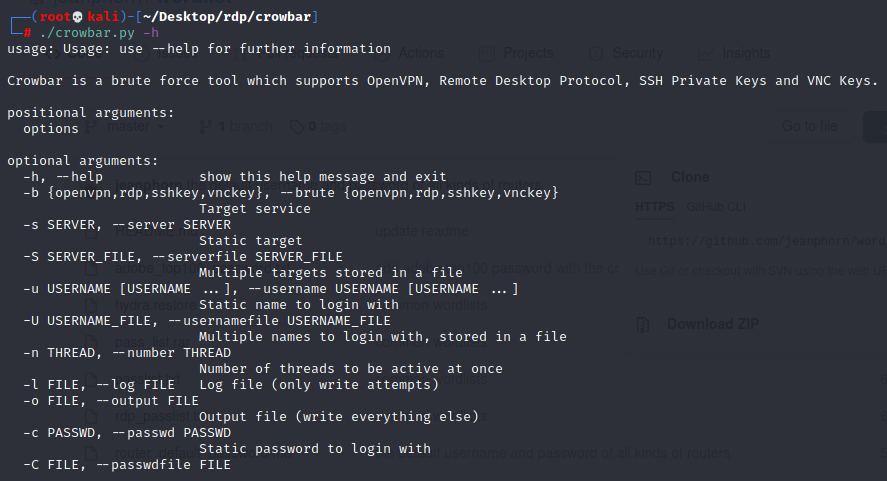
**cd crowbar**

At the prompt, type **ls** to view the contents.



At the prompt type:

**./crowbar.py -h** to view the help menu**.**

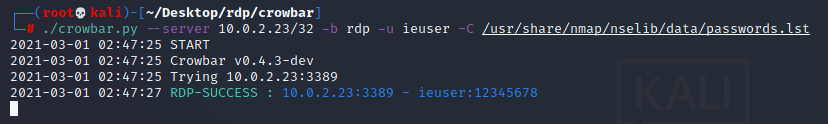


From the help menu, you can add options for the server’s IP address (-s), the username (-u), and the wordlist for the password (-C).

This is the command syntax for our brute force attack. This is my target IP address; yours will differ!

**./crowbar.py --server 10.0.2.23/32 -b rdp -u ieuser -C /usr/share/nmap/nselib/data/passwords.lst**

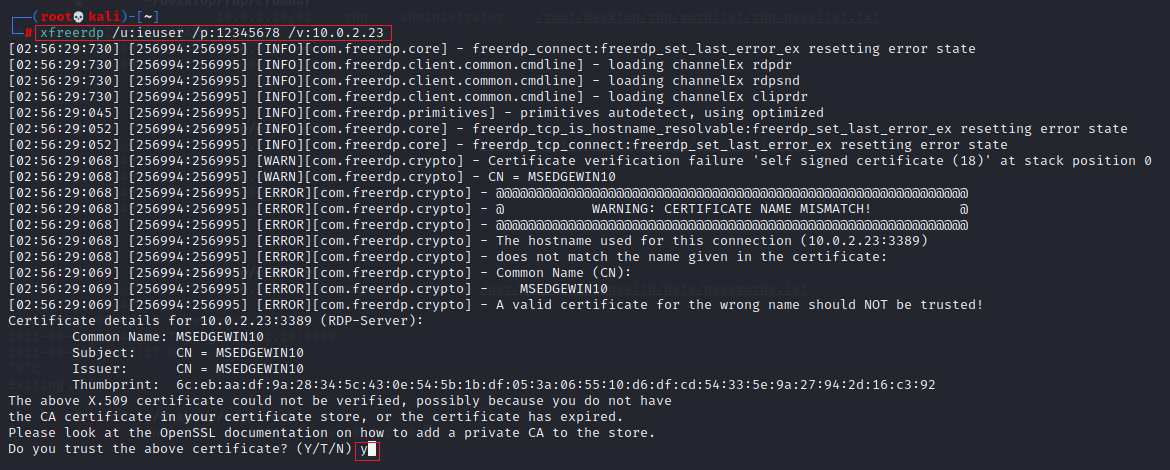
* The --server is the IP address of the target followed by the CIDR for the subnet mask
* The -b is the protocol to use.
* The -u is the name of the user.
* The capital -C is the path and the name of the wordlist used to brute force the password.



We can next attempt to RDP into the remote target using xfreerdp.

**xfreerdp /u:ieuser /p:12345678 /v:10.0.2.23**

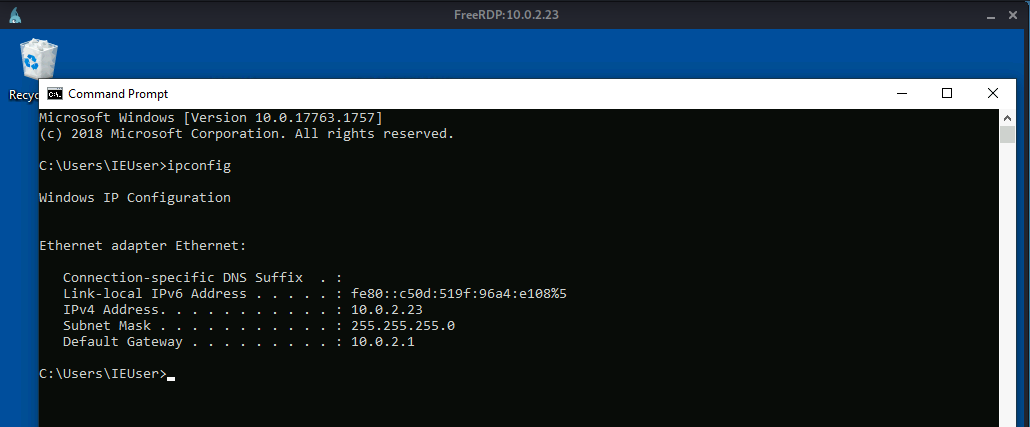




We accept the certificate.

Success!

We have RDP access to the remote target.



**Summary –**

In this lesson, you learned how to perform a brute force attack using RDP. RDP attacks are one of the main entry points when it comes to targeted ransomware operations. Ransomware attacks are getting more targeted to increase effectiveness, and one of the primary attack vectors is the Remote Desktop Protocol (RDP).