

RDP Brute Force Attack_RDP SSH

Last updated by | Kevin Gregoire | Oct 21, 2022 at 9:06 AM PDT

Tags

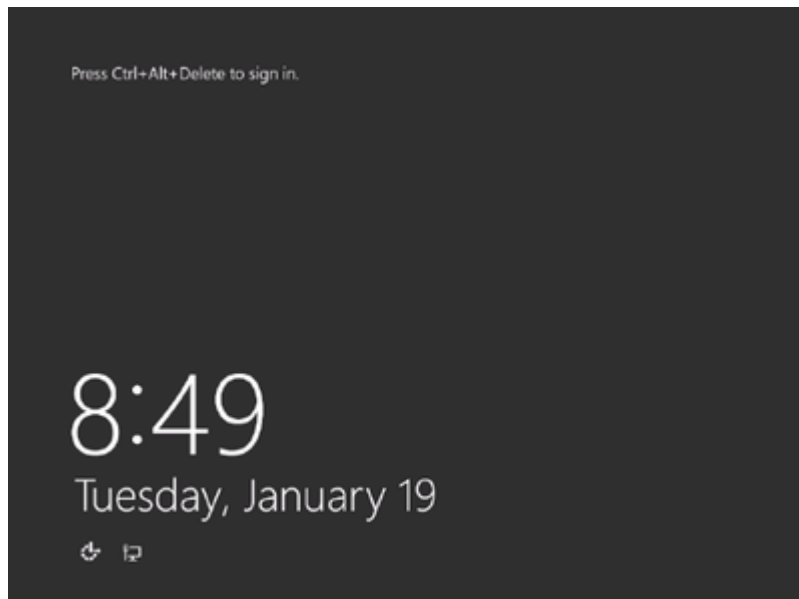
[cw.TSG](#)[cw.RDP-SSH](#)

Contents

- [Symptoms](#)
- [Root Cause Analysis](#)
 - [References](#)
 - [Tracking close code for this volume](#)
- [Customer Enablement](#)
- [Refresher / Training Template](#)
- [Mitigation](#)
- [Need additional help or have feedback?](#)

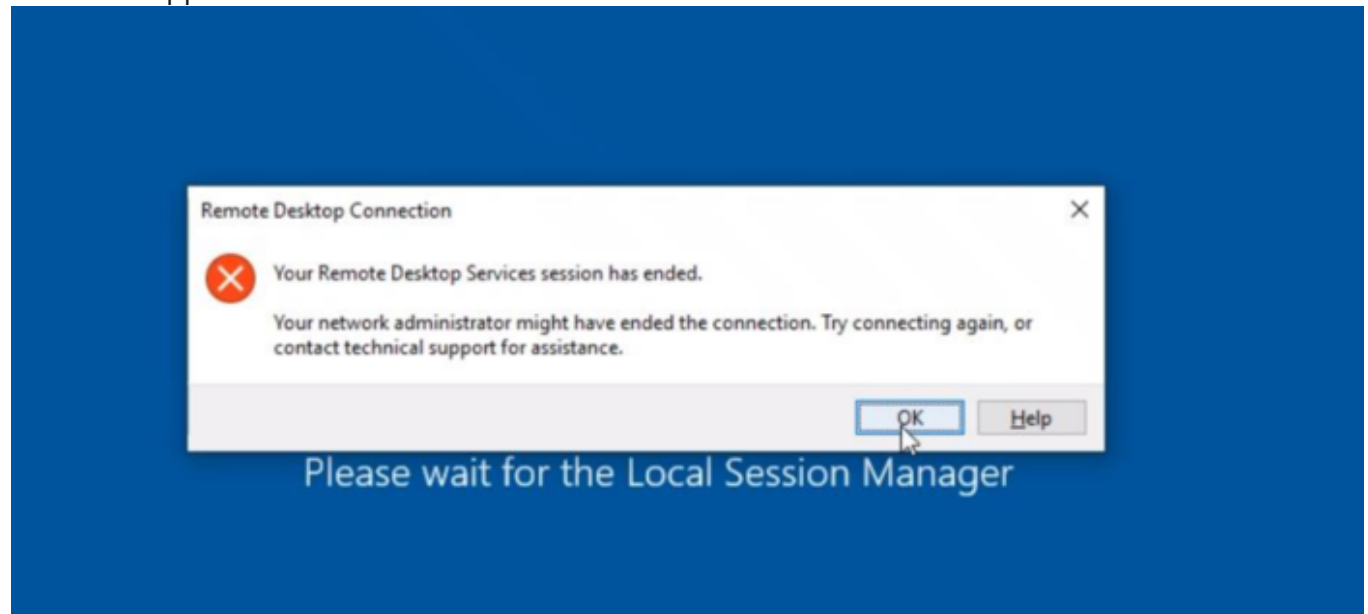
Symptoms

1. The screenshot shows no issues and is on Ctrl+Alt+Del



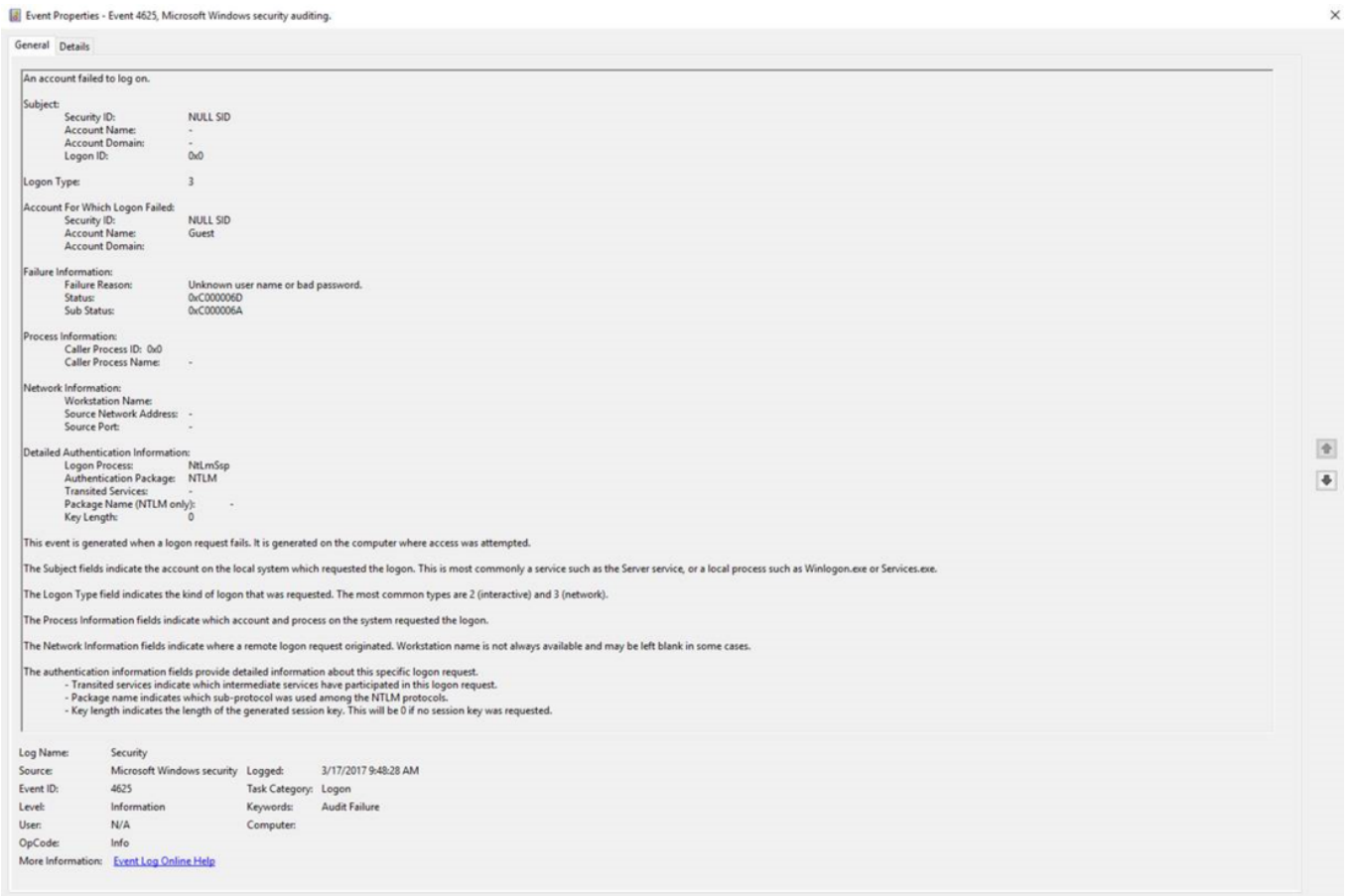
2. When you try to RDP the machine you could get three different behavior:
 1. That the remote machine is unavailable, not responding
 2. RDP windows opens up, get a black screen and after 1min drops
 3. Error message when loading Local Session Manager: **Remote Desktop Services session has ended.**
***Your network administrator might have ended the connection. Try connecting again, or contact

technical support for assistance.***



3. You are unable to RDP using the VIP and you may be able to RDP using the DIP, this will depend if you have a performance spike due to the attack
4. You may find the following events on the windows security event logs as the following:
 1. Events 4625 can be found in windows Security events Logs ;

Level	Date and Time	Source	Event ID	Task Category
Information	3/17/2017 9:48:28 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:48:21 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:48:21 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:48:15 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:48:11 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:48:08 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:48:02 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:55 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:55 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:49 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:43 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:36 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:30 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:29 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:24 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:17 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:10 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:04 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:47:03 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:58 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:51 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:50 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:45 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:41 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:39 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:32 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:26 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:20 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:13 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:12 AM	Microsoft Windows security auditing.	4625	Logon
Information	3/17/2017 9:46:07 AM	Microsoft Windows security auditing.	4625	Logon



2. Event 140 can be found in "Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational events logs " you will find event 140 per each rejected connection:

Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational_1 Number of events: 2,174

Level	Date and Time	Source	Event ID	Task Category
Information	3/17/2017 9:48:08 AM	RemoteDesktopServices-RdpCoreTS	103	RemoteFX module
Information	3/17/2017 9:48:08 AM	RemoteDesktopServices-RdpCoreTS	102	RemoteFX module
Warning	3/17/2017 9:48:08 AM	RemoteDesktopServices-RdpCoreTS	140	RemoteFX module
Information	3/17/2017 9:48:07 AM	RemoteDesktopServices-RdpCoreTS	141	RemoteFX module
Information	3/17/2017 9:48:07 AM	RemoteDesktopServices-RdpCoreTS	65	RemoteFX module
Information	3/17/2017 9:48:07 AM	RemoteDesktopServices-RdpCoreTS	131	RemoteFX module
Information	3/17/2017 9:48:02 AM	RemoteDesktopServices-RdpCoreTS	103	RemoteFX module
Information	3/17/2017 9:48:02 AM	RemoteDesktopServices-RdpCoreTS	102	RemoteFX module
Warning	3/17/2017 9:48:02 AM	RemoteDesktopServices-RdpCoreTS	140	RemoteFX module
Information	3/17/2017 9:48:01 AM	RemoteDesktopServices-RdpCoreTS	141	RemoteFX module
Information	3/17/2017 9:48:01 AM	RemoteDesktopServices-RdpCoreTS	65	RemoteFX module
Information	3/17/2017 9:48:01 AM	RemoteDesktopServices-RdpCoreTS	131	RemoteFX module
Information	3/17/2017 9:47:56 AM	RemoteDesktopServices-RdpCoreTS	103	RemoteFX module
Information	3/17/2017 9:47:56 AM	RemoteDesktopServices-RdpCoreTS	102	RemoteFX module
Information	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	103	RemoteFX module
Information	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	102	RemoteFX module
Warning	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	140	RemoteFX module
Information	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	141	RemoteFX module
Information	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	65	RemoteFX module
Information	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	131	RemoteFX module
Warning	3/17/2017 9:47:55 AM	RemoteDesktopServices-RdpCoreTS	140	RemoteFX module
Information	3/17/2017 9:47:54 AM	RemoteDesktopServices-RdpCoreTS	141	RemoteFX module

Event Properties - Event 140, RemoteDesktopServices-RdpCoreTS

General Details

A connection from the client computer with an IP address of 189.203.136.46 failed because the user name or password is not correct.

Log Name: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
Source: RemoteDesktopServices-RdpCoreTS
Event ID: 140
Level: Warning
User: NETWORK SERVICE
OpCode: ProtocolExchange
More Information: [Event Log Online Help](#)

Logged: 3/17/2017 9:48:08 AM
Task Category: RemoteFX module
Keywords:








Computer:

Copy Close

Root Cause Analysis

The machine is having a brute force RDP attack over the internet, the customer needs to provide more security on his environment.

References

- [Reduce your exposure to brute force attacks from the virtual machine blade](#) 
- [Manage virtual machine access using just in time](#) 
- [Security Best Practices for Windows Azure](#) 
- [Azure Network Security Best Practices](#) 
- [Microsoft cloud services and network security](#) 
- [Control network traffic flow with network security groups](#) 
- [Managing and responding to security alerts in Azure Security Center](#) 

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	Azure Virtual Networks	<i>Routing Azure Virtual Network V3\Connectivity\Cannot connect to virtual machine using RDP or SSH</i>	<i>Root Cause - Windows Azure\Virtual Network\NSG\Configuration\Customer misconfiguration</i>	

To know how to flag a bug on a case please refer to [How to do Proper Case Coding](#)

Customer Enablement

- [Cannot RDP into Azure VM because of a brute force attack](#) ☑
- [An internal error occurs when you try to connect to an Azure VM through Remote Desktop](#) ☑

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.




Mitigation

In this scenario, we should suggest the customer to reinforce the security on their environment. This could be achieved in multiple ways:

1. The customer could review the NSG rules. You can either create or update an existing NSG to make it more restricted allowing access only to an IP range (customer's office network) and/or denying access to the rest. Please review the article [Control network traffic flow with network security groups](#) ☑
 - For the inbound RDP (TCP Port 3389) rule, if the Source IP Address is set to "Any" or " * " while a Public IP is assigned, then the rule is considered open and the VM is vulnerable.
 - You can also restrict the RDP port to the current customer's IP address (they can quickly find it by searching Bing for "my ip") and test RDP access again.
2. You can also restrict the access to the VMs using RBACs, please refer to [Use Role-Based Access Control to manage access to your Azure subscription resources](#) ☑
3. Another option is by using just in time (JIT) access like this article explains [Manage virtual machine access using just in time](#) ☑
4. You can also put a the VM behind a Load Balancer and changing the public RDP port to a high (five digits) port. Refer this article, under *Access Via Public Load Balancer* section [External RDP Access To Azure VM](#) ☑
5. An additional solution is [Azure Bastion](#) ☑, which provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS, without requiring a public IP address.

Need additional help or have feedback?

<i>To engage the Azure RDP-SSH SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the RDP-SSH SMEs  for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the RDP-SSH Feedback form to submit detailed feedback on improvements or new content ideas for RDP-SSH.</p> <p>Please note the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.</p>	<p>Use the RDP-SSH Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>