

RDP Protection Readme

Overview

RDP exposed to the internet is problematic.

The general rule should be: no RDP without VPN, even if protected by an MFA product (like DUO). The door knock occurs before MFA, can lock accounts, and stress the winlogon process in a DDOS manner. Check your Windows event log in the security section for 4625 events to see if this is happening.

RDP Protection checks Event log for failed access attempts and blocks those IPs using Windows firewall. Successful attempts can be added to the allow list automatically. Blocks and allows are maintained in a CSV file, so you can whitelist IP numbers.

```
RDP Protection.ps1 v2023-12-10      Computer:  User:  PSver:5.1

- Checks Event log for failed access attempts and blocks those IPs using Windows
- Successful attempts can be added to the allow list automatically
- blocks and allows are maintained in a CSV file

[Options]
-Mode Normal

-----

[Status]
OK: Enabled Network adapter 'Ethernet0 Network (Internet) NetworkCategory Private'
OK: Firewall is active
OK: RDP port is 3389
OK: RDP service is running
OK: DUO is enabled
-----

[Local admin accounts]
Admin 1:  [Vulnerable account name]
Admin 2: 
Admin 3: 
WARNING: (202) Vulnerable local admin accounts: Administrator
-----

[Program Settings] (from RDP Protection Settings.csv)
block_aftertries: 5
  blocksubnet: yes
  lookbackmins: 1440 (1d)
  allowaftermins: 1440 (1d)
  autoallow: yes
  last_rundate: 04/27/2024 14:32:08 (44s ago)
-----
```

How to Install

Right click *RDP Protection.cmd* and Run as Admin to install:

- Creates a C:\RDP Protection folder with all the required files
- Schedules a task every 2 hours that runs the protection process
- The protection process looks in the Event log for 4625 events and, if the same IP fails 5 times, the IP is added to a Windows Firewall block rule.
- Information about the offending IP is pulled from internet resource sites
- A CSV file keeps track of blocked addresses
- Vulnerable Local admin accounts are displayed – make sure these are protected with good passwords etc

How to Use it

Once it's scheduled, right click *RDP Protection.cmd* and Run as Admin to check for intruders on demand.
Look in C:\RDP Protection for logs, blocks, etc.

Uninstall

Right click *RDP Protection -mode Uninstall.cmd* and Run as Admin to uninstall




Removes the scheduled task

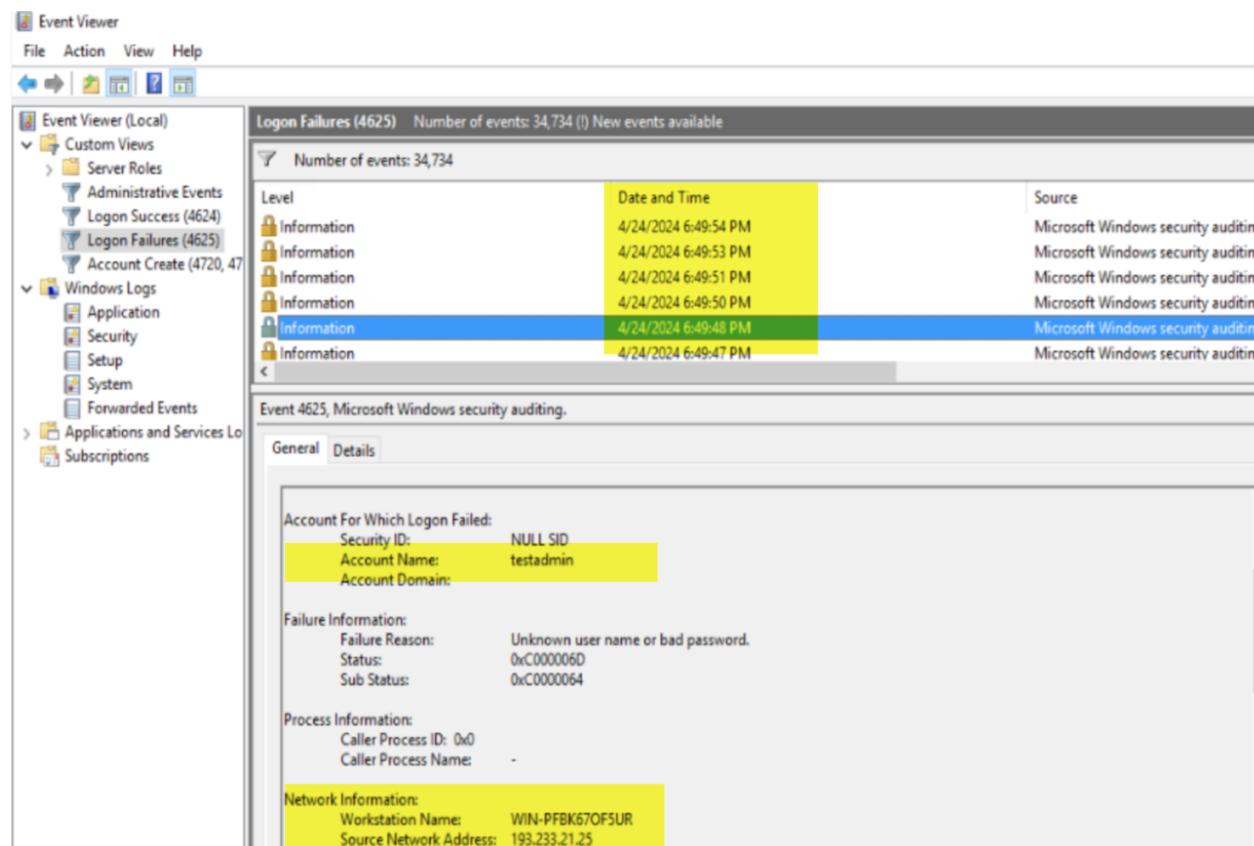
Removes the C:\RDP Protection folder

Event Log

The Windows Event log (Security) keeps track of logon successes, failures and account changes.

In Event Viewer, import the 3 .xml files which contain the correct view filters for these events.

-  Event Viewer (4624 Successes) Import.xml
-  Event Viewer (4625 Failures) Import.xml
-  Event Viewer (Account Creations) Import.xml



The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Event Viewer (Local)' tree with 'Logon Failures (4625)' selected under 'Windows Logs > Security'. The right pane shows a list of 34,734 events. The selected event, 4625, is highlighted in blue. Below the list, the 'Details' tab is active, showing the following information:

Account For Which Logon Failed:	
Security ID:	NULL SID
Account Name:	testadmin
Account Domain:	

Failure Information:	
Failure Reason:	Unknown user name or bad password.
Status:	0xC000006D
Sub Status:	0xC0000064

Process Information:	
Caller Process ID:	0x0
Caller Process Name:	-

Network Information:	
Workstation Name:	WIN-PFBK67OF5UR
Source Network Address:	193.233.21.25

[end of file]