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

Succesful attempts can be added to the allow list automatically blocks and allows are maintained in a CSV file, so you can whitelist IP numbers.

A computer screen shot of a black screen

Description automatically generated

# 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.

A number of words on a white background

Description automatically generated

A screenshot of a computer

Description automatically generated

[end of file]