

# Easy to implement security tips

for Citrix, AVD, Windows365 and Omnissa



# Stefan Dingemanse



**Focus**  
Modern Workplace  
Consultant/Architect at Brainpulse IT

**From**  
  
The Netherlands

**My blog**  
<https://stefandingemanse.com>



## Communities

Azure Thursday  
Dutch Virtual Desktop User Group

## Hobbies

Hyrox / Crossfit 

## Contact

Stefan@brainpulse.it





# Patrick van den Born



## Focus

End User Computing

DevOps way of working



## From

The Netherlands



## My blog

[www.detechnischejongens.nl](http://www.detechnischejongens.nl)

[www.go-euc.com](http://www.go-euc.com)



## Communities

GO-EUC

Dutch Virtual Desktop User Group

Microsoft and Citrix

## Hobbies

CrossFit

Weightlifting

Sim racing

## Contact

[patrick@detechnischejongens.nl](mailto:patrick@detechnischejongens.nl)





# Agenda

- Real World Scenarios
- What are the risks
- Easy to implement security tips
- Recap
- Questions



Personal – Real world scenario

# Personal – Real world scenario



EUC Environments



Application configuration



Easy tips

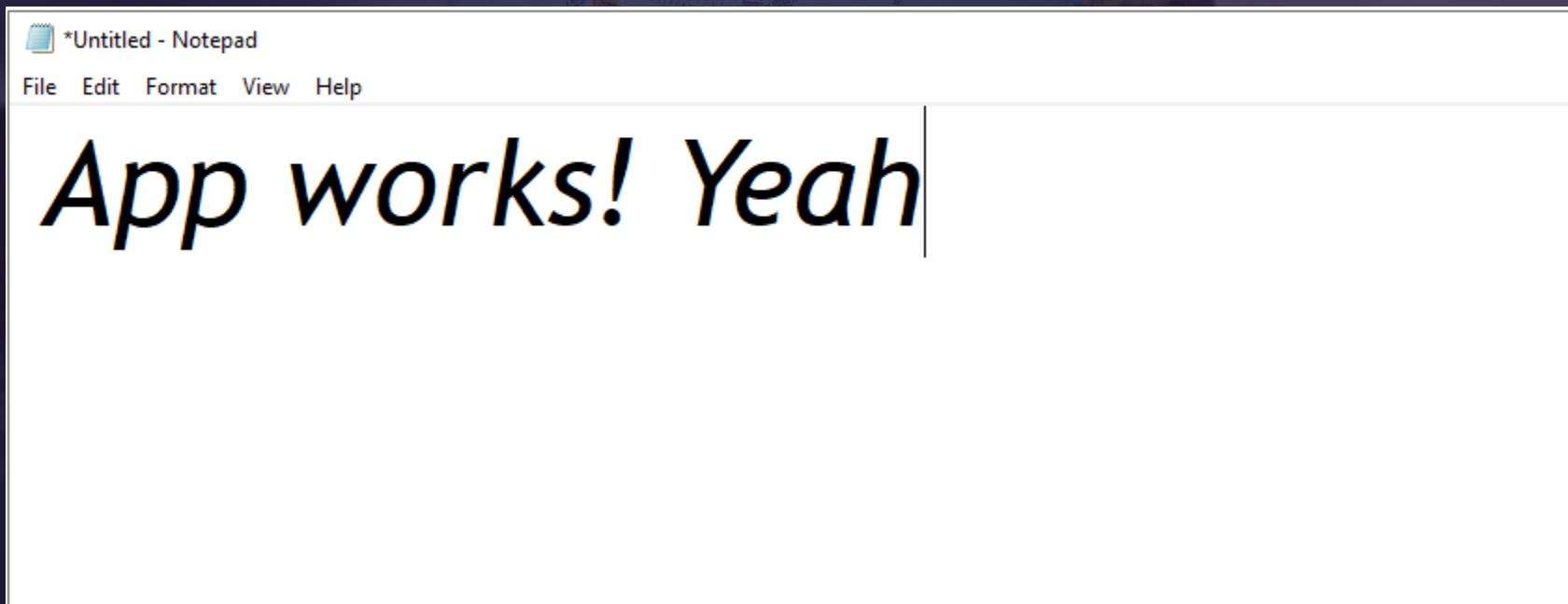


Session Host defense

# Customer example

Virtual Apps							
Linked Group Policy Objects		Group Policy Inheritance		Delegation			
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	RDS2019 - CALs	No	Yes	User configuratio...	None	23-11-2021 ...	vandenbor...
2	Application - Notepad Fonts	No	Yes	Computer config...	None	20-9-2024 1...	vandenbor...

# Customer example

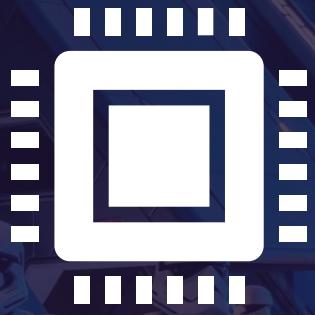




Security findings from the field



Scripting



OS



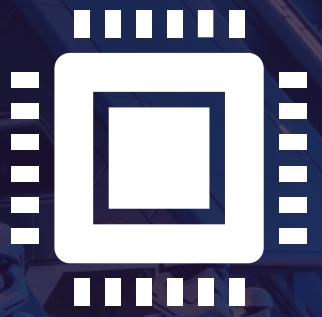
Applications

# Security findings from the field



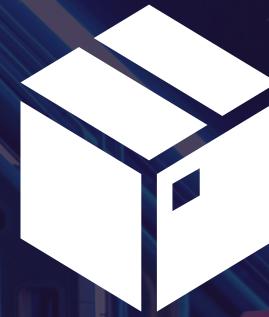
## Scripting

Powershell v2 enabled  
Powershell full language mode



## OS

Cached credentials  
User write rights  
Identical local admin passwords  
Network communication  
Outbound internet firewall  
Windows updates strategy



## Applications

No application whitelisting  
Outdated applications  
Internet Explorer 11  
No virus scanners or EDR/XDR



What are the risks?



Cyber  
war



Internet  
facing



Lateral  
movement



Ransomware  
Delivery  
Protocol

# Windows Privilege Escalation Awesome Scripts

https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS

Product Solutions Resources Open Source Enterprise Pricing

peass-ng / PEASS-ng Public

Sponsor Notifications Fork 3.1k Star 15.8k

Code Issues 24 Pull requests 1 Actions Projects Security Insights

Files

master

Go to file

.github build\_lists linPEAS metasploit parsers winPEAS

winPEAS

winPEASbat winPEASExe winPEASps1 README.md .gitignore CONTRIBUTING.md LICENSE README.md TODO.md

PEASS-ng / winPEAS /

carlospolop f2 ✓ b3bcfa4 · 3 weeks ago History

Name	Last commit message	Last commit date
...		
winPEASbat	WinPEASS Big Update	3 weeks ago
winPEASExe	f2	3 weeks ago
winPEASps1	WinPEASS Big Update	3 weeks ago
README.md	WinPEASS Big Update	3 weeks ago

README.md

## Windows Privilege Escalation Awesome Scripts



Check the Local Windows Privilege Escalation checklist from [book.hacktricks.xyz](#)

Check more information about how to exploit found misconfigurations in [book.hacktricks.xyz](#)

### Quick Start

Find the latest versions of all the scripts and binaries in [the releases page](#).

### WinPEAS Flavours

- Link to WinPEAS C# .exe project (Net >= 4.5.2 required)

# Windows Privilege Escalation Awesome Scripts

```
PS Select Command Prompt
[?] Basic System Information
[*] Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#exploits
[*] Loading Processor Information ...

OS Name: Microsoft Windows 10 Pro
OS Version: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~2112 Mhz
System Type: x64-based PC
Hostname: DESKTOP-NTKR9E3
ProductName: Windows 10 Pro
EditionID: Professional
ReleaseId: 2004
BuildBranch: vb_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 2
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC-05:00) Eastern Time (US & Canada)
IsVirtualMachine: True
Current Time: 8/10/2024 11:55:44 AM
HighIntegrity: False
PartOfDomain: False
Hotfixes: KB5006365, KB4537759, KB4557968, KB5033052, KB4556803,
[?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
[*] OS Version: 2004 (19041)
[*] Enumerating installed KBs...
[!] CVE-2020-1013 : VULNERABLE
[>] https://www.gosecure.net/blog/2020/09/08/wsus-attacks-part-2-cve-2020-1013-a-windows-10-local-privilege-escalation-1-day/
[*] Finished. Found 1 potential vulnerabilities.
```



Image adjustments

# Image adjustments

Advanced Security Settings for Local Disk (C:)

Name: C:\  
Owner: TrustedInstaller [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Principal	Type	Access	Inherited from	Applies to
Administrators (DESKTOP...)	Allow	Full control	None	This folder, subfolders and files
SYSTEM	Allow	Full control	None	This folder, subfolders and files
Users (DESKTOP-RCL8FSE...)	Allow	Read & execute	None	This folder, subfolders and files
Authenticated Users	Allow	Modify	None	Subfolders and files only
Authenticated Users	Allow	Create folders / append data	None	This folder only
Account Unknown(\$-1-1...)	Allow	Special	None	This folder only

[Change permissions](#) [View](#)

OK Cancel Apply

Remove default rights for Authenticated Users

# Image adjustments

```
# Adjust C-drive permissions
Write-Host "##[C-Drive]Retrieving security principal for SID S-1-5-11 (NT AUTHORITY\Authenticated Users)"
$SID = New-Object System.Security.Principal.SecurityIdentifier("S-1-5-11")
$user = $SID.Translate([System.Security.Principal.NTAccount])
Write-Host "##[C-Drive]NT AUTHORITY\Authenticated Users group name is ($($User.Value))"
Write-Host "##[command][C-Drive]Setting C-Drive permissions"

$aclroot = Get-Acl -Path "C:\"
$accessToRemove = @('AppendData', '-536805376')

foreach ($access in $accessToRemove) {
    $removeAcl = $aclroot.Access | Where-Object { $_.IdentityReference -like $($User.Value) -and
$_.FileSystemRights -like $access }
    if ($removeAcl) {
        $aclroot.RemoveAccessRule($removeAcl)
        Write-Host "##[C-Drive]Removed [ $($User.Value) ] with access [ $access ]"
    }
}

Write-Host "##[C-Drive]Start applying new ACL on C-Drive - This might take a while"
)null = Set-Acl -Path "C:\" -AclObject $aclroot
Write-Host "[C-Drive]Done!"
```

# Image adjustments

```
#Disable Cached Logons on server
Write-Host "##[command] [Cached-Credentials] Disabling Cached Credentials"
$securityCachedLogonsCount = [ordered] @{
    RegistryPath = "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
    RegistryName = "CachedLogonsCount"
    RegistryValue = "0"
    RegistryType = "String"
}
$securityCachedLogonsCount | Format-Table -AutoSize | Write-output
Set-RegistryValue @securityCachedLogonsCount
Write-Host "[Cached-Credentials] done"
```

# Image adjustments

```
$featureVariables = [ordered]@{  
    Online      = $true  
    FeatureName = "MicrosoftWindowsPowerShellV2Root"  
}  
  
#Logging  
Write-Host "Disable: $($featureVariables.FeatureName)"  
$featureVariables | Format-Table -AutoSize | Write-output  
  
#Disable Windows Feature  
Disable-WindowsOptionalFeature @featureVariables
```

# Image adjustments

```
$featureVariables = [ordered]@{  
    Online      = $true  
    FeatureName = "Internet-Explorer-Optional-amd64"  
}  
  
#Logging  
Write-Host "Disable: $($featureVariables.FeatureName)"  
$featureVariables | Format-Table -AutoSize | Write-output  
  
#Disable Windows Feature  
Disable-WindowsOptionalFeature @featureVariables
```

# Consistent Image Release Strategy

Citrix Machine Creation Services  
Citrix Provisioning Services

Azure Virtual Desktop Session Host Configuration

Omnissa Linked Clones

Home > Azure Virtual Desktop > Create a host pool

Resource group \* rg-HVC-AVD-DEV-Win11MS-builder  
Create new

Host pool name \* aaaa

Location \* East US  
Metadata will be stored in Azure geography associated with (US) East US. [Learn more](#)

Validation environment  No  Yes

Preferred app group type \* Desktop

Host pool details  
Define how session hosts in this host pool will be created, managed, and assigned.

Host pool type \* Pooled  
If you select pooled, users can maintain their personalization and user data with FSLogix. [Learn more](#)

Create Session Host Configuration \*  No  
You manage the lifecycle of the session hosts and don't use Azure Virtual Desktop to update them.

Yes (Preview)  
Session hosts are created and updated based on the configuration you define. You won't be able to manually add session hosts using a registration key.

Load balancing algorithm Breadth-first

Max session limit Max # of users per session host

[Review + create](#) < Previous Next: Session hosts >



# Creating Confidence in the Connected World™

At CIS®, we're harnessing the power of the global IT community to safeguard public and private organizations against cyber threats. Join us.

World-Renowned Best Practices and Expert Communities



The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.



## Microsoft

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.



against cybersecurity threats.



Lower the attack surface



The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.



## Microsoft

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.



## DoD CYBER EXCHANGE PUBLIC

STIGs are developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). They offer a set of guidelines for various operating systems, including Windows and Linux, to secure an organization's assets against cybersecurity threats.

CIS benchmarks provide two levels of security settings:

- **Level 1** recommends essential basic security requirements that can be configured on any system and should cause little or no interruption of service or reduced functionality.
- **Level 2** recommends security settings for environments requiring greater security that could result in some reduced functionality.



The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.



## Microsoft

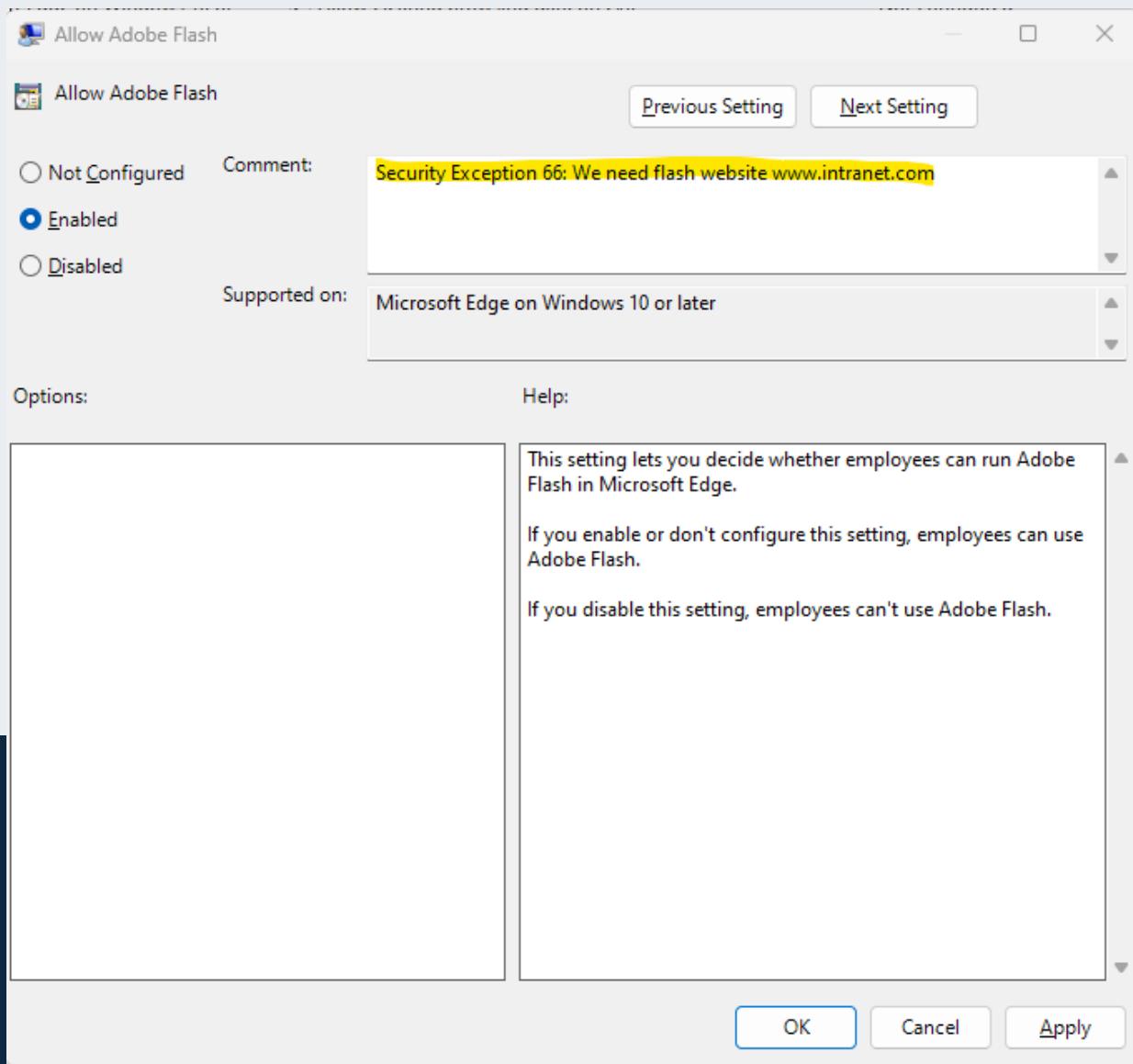
A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

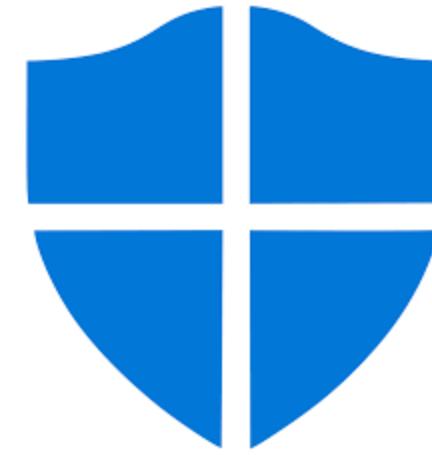


## DoD CYBER EXCHANGE PUBLIC

STIGs are developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). They offer a set of guidelines for various operating systems, including Windows and Linux, to secure an organization's assets against cybersecurity threats.

1AVD_PROD_COMP_Settings	All Computer related policy settings combined	
2AVD_PROD_USER_Settings	All User related policy settings combined	
3AVD_PROD_AppLocker	AppLocker Policy	
<b>4AVD_PROD_CIS_Exceptions</b>	<b>User/Computer Exceptions on General Cis</b>	<b>Enforced</b>
5AVD_PROD_CIS	CIS Policy Microsoft Windows, Office, Edge, RemoteApps (unchanged)	





Microsoft Security Baselines and CIS Remote Desktop Protocol



The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.



## Microsoft

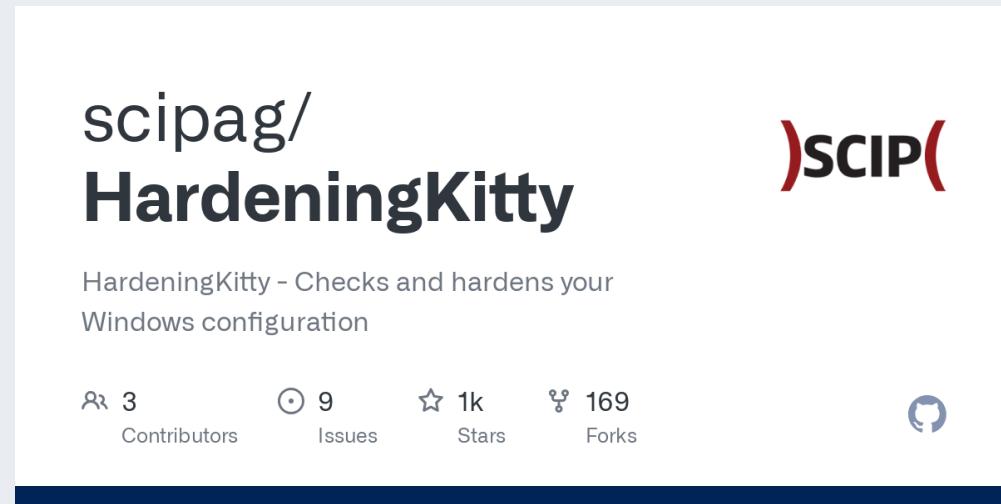
A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.



STIGs are developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). They offer a set of guidelines for various operating systems, including Windows and Linux, to secure an organization's assets against cybersecurity threats.



Validate and test



<https://github.com/scipag/HardeningKitty>



Good Old PolicyAnalyzer



Vulnerability Scanner



Application whitelisting the easy way

# Application whitelisting the easy way

This app has been blocked by your system administrator.

Contact your system administrator for more info.

[Copy to clipboard](#)

[Close](#)



Allow applications



Pen testers



Abnormally detection



User writable folders

# Application whitelisting the easy way

The screenshot shows a Microsoft Edge browser window with a dark theme. The address bar displays the URL <https://github.com/microsoft/AaronLocker>. The page content is the GitHub repository for `AaronLocker`, which is described as "Robust and practical application control for Windows". The repository has 5 branches and 0 tags. The main branch is selected. The repository has 72 commits, with the most recent being a merge pull request from `microsoft/users/GitHubPolicyService`. Other commits include updates to `README.md`, `LICENSE`, and `SECURITY.md`. The repository has 593 stars, 58 watchers, and 72 forks. There are sections for **About**, **Releases**, and **Packages**, both of which are currently empty.

**About**

Robust and practical application control for Windows

[Readme](#) [MIT license](#) [Code of conduct](#) [Security policy](#) [Activity](#) [Custom properties](#)

593 stars 58 watching 72 forks

[Report repository](#)

**Releases**

No releases published

**Packages**

No packages published

**Overview**

AaronLocker is designed to make the creation and maintenance of robust, strict, application control for AppLocker and Windows Defender Application Control (WDAC) as easy and practical as possible. The entire solution involves a small number of PowerShell scripts. You can easily customize rules for your

# Application whitelisting the easy way

```
Administrator: PowerShell x Administrator: Windows Pow x + v
PS D:\AaronLocker\AaronLocker> .\Create-Policies.ps1
Get EXE files to DenyList for later processing...
Get authorized safe paths for later processing...
Computer is not domain-joined; not adding path for DC shares.
Get 'unsafe' user-writable paths for later processing...
Processing additional safe paths to AllowList...
WARNING: Cannot verify path ; adding to rule set as is.
WARNING: Cannot verify path ; adding to rule set as is.
WARNING: Cannot verify path ; adding to rule set as is.
WARNING: Cannot verify path ; adding to rule set as is.
WARNING: Cannot verify path ; adding to rule set as is.
WARNING: Cannot verify path ; adding to rule set as is.
Creating rules for trusted publishers...
    Microsoft Teams: Signer/product rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/MICROSOFT TEAMS
    Microsoft-signed MSI files: Signer rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US
    Microsoft-signed script files: Signer rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US
    Allow selected files from %OSDRIVE%\~BT\SOURCES during Windows upgrade: Signer/product/file rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/MICROSOFT® WINDOWS® OPERATING SYSTEM/GENERALTEL.DLL
    Allow selected files from %OSDRIVE%\~BT\SOURCES during Windows upgrade: Signer/product/file rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/MICROSOFT® WINDOWS® OPERATING SYSTEM/WDSCORE.DLL
    Allow selected files from %OSDRIVE%\~BT\SOURCES during Windows upgrade: Signer/product/file rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/MICROSOFT® WINDOWS® OPERATING SYSTEM/AEINV.DLL
    MS Edge content protection: Signer/product rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/WIDEVINE CONTENT DECRYPTION MODULE
    AVDRemoteClient: Signer/product/file rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/*/RDPNANOTRANSPORT.DLL
    MSVC runtime DLL: Signer/product/file rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/MICROSOFT® VISUAL STUDIO® 2005/MSVCP80.DLL
    MSVC runtime DLL: Signer/product/file rule for O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US/MICROSOFT® VISUAL STUDIO® 2005/MSVCR80.DLL
```

# Application whitelisting the easy way

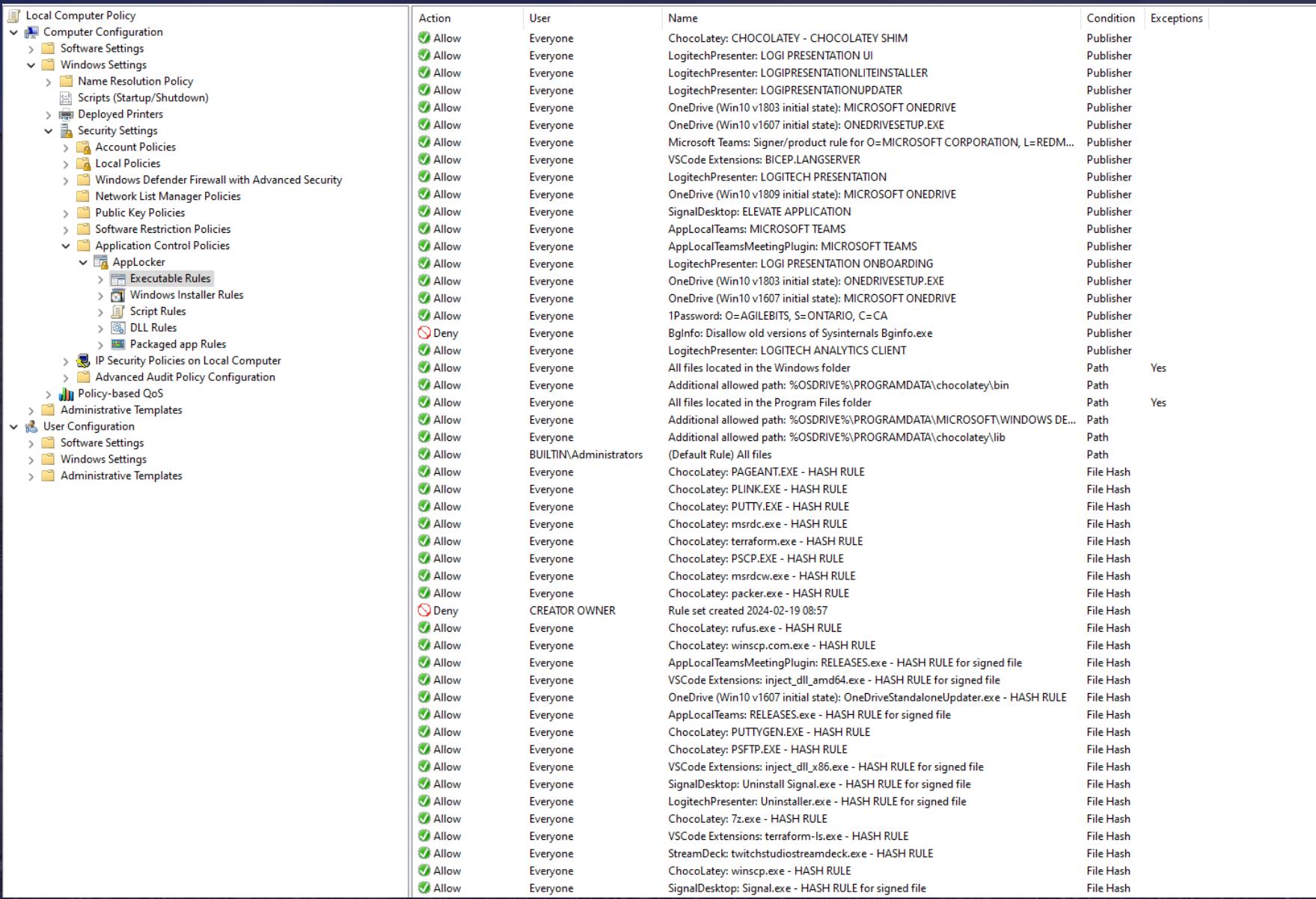
```
Administrator: PowerShell      Administrator: Windows Pow + | - X
ID_ALLOW_A_66B_APPLOCALTEAMS...
ID_ALLOW_A_66C_APPLOCALTEAMS...
ID_ALLOW_A_699_CHOCOLATEY_1_1
ID_ALLOW_A_69A_CHOCOLATEY_1_1
ID_ALLOW_A_69B_CHOCOLATEY_1_1
ID_ALLOW_A_69C_CHOCOLATEY_1_1
ID_ALLOW_A_69D_CHOCOLATEY_1_1
Updating PolicyName, PolicyVersion, and TimeStamp...
Copying D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Allow-Audit.xml to D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Allow-Enforce.xml...
Setting PolicyName for D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Allow-Enforce.xml to WDAC AaronLocker Allow list - Enforced...
Saving D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Deny-Audit.xml after setting PolicyID info from previous run...
Merging custom rule sets into new policy file...
    Merging MergeRules-Dynamic\WDACRules-DenyRules.xml
ID_ALLOW_A_1_0
ID_ALLOW_A_2_0
ID_SIGNER_F_BFE_1
ID_SIGNER_F_BFF_1
ID_SIGNER_F_BF9_1
ID_SIGNER_F_BFA_1
Updating PolicyName, PolicyVersion, and TimeStamp...
Copying D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Deny-Audit.xml to D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Deny-Enforce.xml...
Setting PolicyName for D:\AaronLocker\AaronLocker\Outputs\WDACRules-20240219-1200-Deny-Enforce.xml to WDAC AaronLocker Deny list - Enforced...

PS D:\AaronLocker\AaronLocker>
```

# Application whitelisting the easy way

Name	Date modified	Type	Size
AppLockerRules-20240621-1429-Audit.xml	21/06/2024 14:33	XML Source File	518 KB
AppLockerRules-20240621-1429-Enforce.xml	21/06/2024 14:33	XML Source File	518 KB
AppLockerRules-20240621-1643-Audit.xml	21/06/2024 16:53	XML Source File	518 KB
AppLockerRules-20240621-1643-Enforce.xml	21/06/2024 16:53	XML Source File	518 KB
AppLockerRules-20240819-1042-Audit.xml	19/08/2024 10:46	XML Source File	547 KB
AppLockerRules-20240819-1042-Enforce.xml	19/08/2024 10:46	XML Source File	547 KB
WDACRules-20240621-1429-Allow-Audit.xml	21/06/2024 14:47	XML Source File	545 KB
WDACRules-20240621-1429-Allow-Enforce.xml	21/06/2024 14:47	XML Source File	545 KB
WDACRules-20240621-1429-Deny-Audit.xml	21/06/2024 14:47	XML Source File	9 KB
WDACRules-20240621-1429-Deny-Enforce.xml	21/06/2024 14:47	XML Source File	9 KB
WDACRules-20240621-1643-Allow-Audit.xml	24/06/2024 09:17	XML Source File	545 KB
WDACRules-20240621-1643-Allow-Enforce.xml	24/06/2024 09:17	XML Source File	545 KB
WDACRules-20240621-1643-Deny-Audit.xml	24/06/2024 09:17	XML Source File	9 KB
WDACRules-20240621-1643-Deny-Enforce.xml	24/06/2024 09:17	XML Source File	9 KB
WDACRules-20240819-1042-Allow-Audit.xml	19/08/2024 10:58	XML Source File	569 KB
WDACRules-20240819-1042-Allow-Enforce.xml	19/08/2024 10:58	XML Source File	568 KB
WDACRules-20240819-1042-Deny-Audit.xml	19/08/2024 10:58	XML Source File	9 KB
WDACRules-20240819-1042-Deny-Enforce.xml	19/08/2024 10:58	XML Source File	9 KB

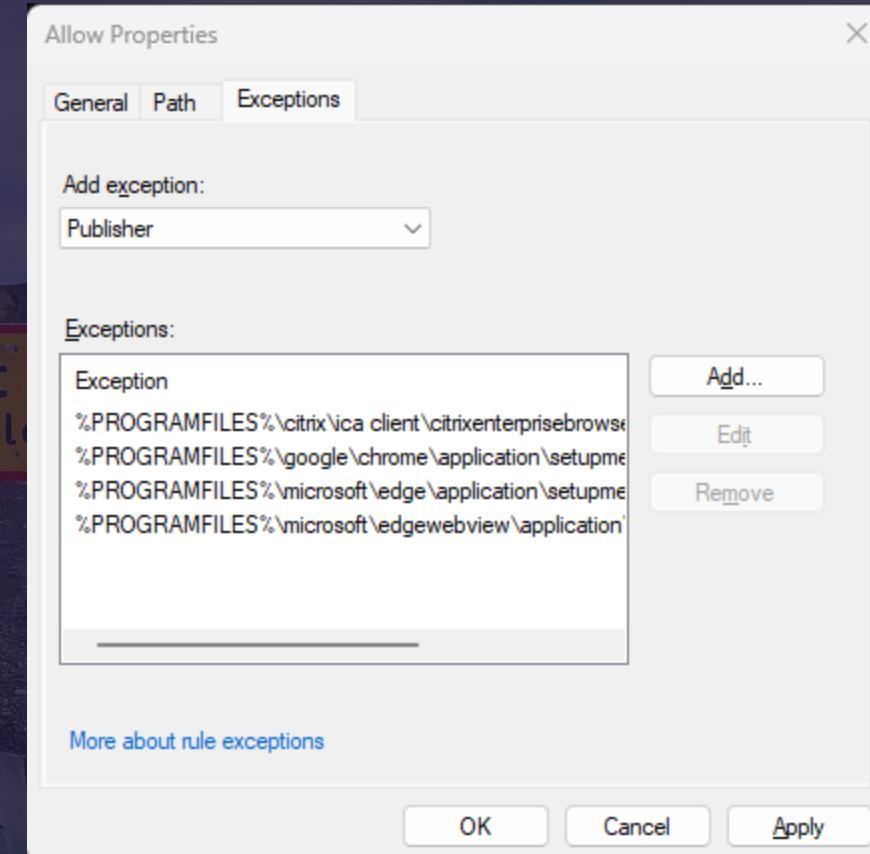
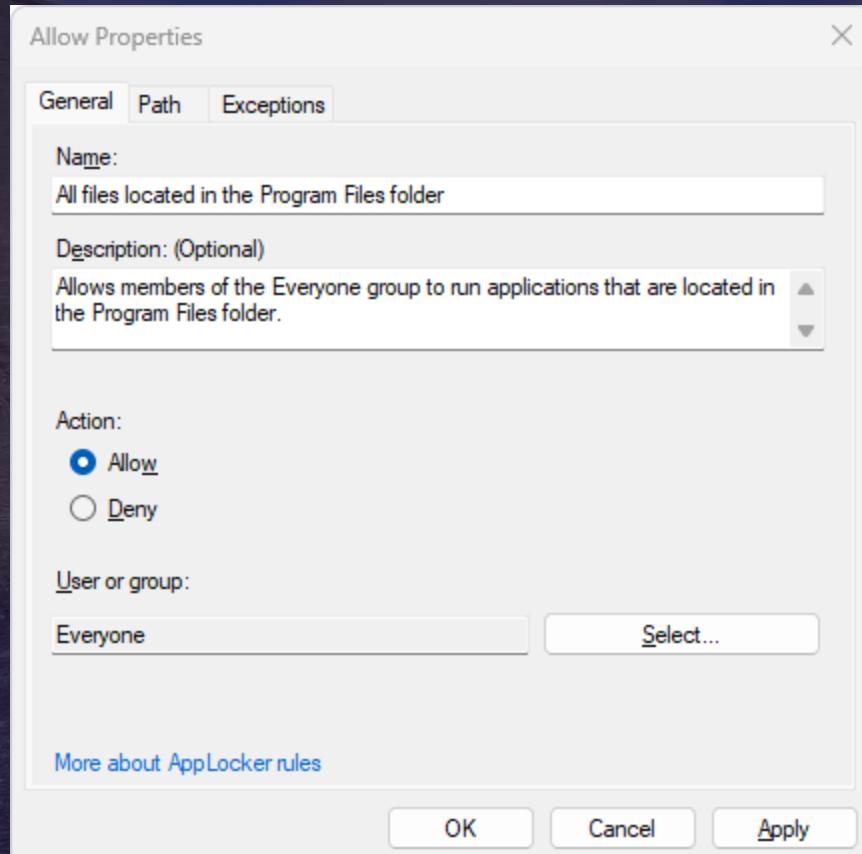
# Application whitelisting the easy way



The screenshot shows the Windows Local Computer Policy Editor window. On the left, the navigation pane displays the policy structure under 'Local Computer Policy' (Computer Configuration, Software Settings, Windows Settings, Security Settings, Application Control Policies, User Configuration). The 'AppLocker' node under 'Application Control Policies' is expanded, showing categories like Executable Rules, Windows Installer Rules, Script Rules, DLL Rules, and Packaged app Rules. The main pane on the right lists a large number of whitelisted application entries, each with columns for Action (Allow/Deny), User (Everyone or BUILTIN\Administrators), Name (the application path), Condition (Publisher or Path), and Exceptions (Yes or No).

Action	User	Name	Condition	Exceptions
Allow	Everyone	ChocoLatey: CHOCOLATEY - CHOCOLATEY SHIM	Publisher	
Allow	Everyone	LogitechPresenter: LOGI PRESENTATION UI	Publisher	
Allow	Everyone	LogitechPresenter: LOGIPRESENTATIONLITEINSTALLER	Publisher	
Allow	Everyone	LogitechPresenter: LOGIPRESENTATIONUPDATER	Publisher	
Allow	Everyone	OneDrive (Win10 v1803 initial state): MICROSOFT ONEDRIVE	Publisher	
Allow	Everyone	OneDrive (Win10 v1607 initial state): ONEDRIVESETUP.EXE	Publisher	
Allow	Everyone	Microsoft Teams: Signer/product rule for O=MICROSOFT CORPORATION, L=REDM...	Publisher	
Allow	Everyone	VSCode Extensions: BICEP.LANGSERVER	Publisher	
Allow	Everyone	LogitechPresenter: LOGITECH PRESENTATION	Publisher	
Allow	Everyone	OneDrive (Win10 v1809 initial state): MICROSOFT ONEDRIVE	Publisher	
Allow	Everyone	SignalDesktop: ELEVATE APPLICATION	Publisher	
Allow	Everyone	AppLocalTeams: MICROSOFT TEAMS	Publisher	
Allow	Everyone	AppLocalTeamsMeetingPlugin: MICROSOFT TEAMS	Publisher	
Allow	Everyone	LogitechPresenter: LOGI PRESENTATION ONBOARDING	Publisher	
Allow	Everyone	OneDrive (Win10 v1803 initial state): ONEDRIVESETUP.EXE	Publisher	
Allow	Everyone	OneDrive (Win10 v1607 initial state): MICROSOFT ONEDRIVE	Publisher	
Deny	Everyone	1Password: O=AGILEBITS, S=ONTARIO, C=CA	Publisher	
Allow	Everyone	BglInfo: Disallow old versions of Sysinternals Bginfo.exe	Publisher	
Allow	Everyone	LogitechPresenter: LOGITECH ANALYTICS CLIENT	Publisher	
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	Everyone	Additional allowed path: %OSDRIVE%\PROGRAMDATA\chocolatey\bin	Path	
Allow	Everyone	All files located in the Program Files folder	Path	Yes
Allow	Everyone	Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DE...	Path	
Allow	BUILTIN\Administrators	Additional allowed path: %OSDRIVE%\PROGRAMDATA\chocolatey\lib	Path	
Allow	Everyone	(Default Rule) All files	Path	
Allow	Everyone	ChocoLatey: PAGEANT.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PLINK.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PUTTY.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: msrdc.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: terraform.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PSCP.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: msrdcw.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: packer.exe - HASH RULE	File Hash	
Deny	CREATOR OWNER	Rule set created 2024-02-19 08:57		
Allow	Everyone	ChocoLatey: rufus.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: winscp.com.exe - HASH RULE	File Hash	
Allow	Everyone	AppLocalTeamsMeetingPlugin: RELEASES.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	VSCode Extensions: inject_dll_amd64.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	OneDrive (Win10 v1607 initial state): OneDriveStandaloneUpdater.exe - HASH RULE	File Hash	
Allow	Everyone	AppLocalTeams: RELEASES.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	ChocoLatey: PUTTYGEN.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PSFTP.EXE - HASH RULE	File Hash	
Allow	Everyone	VSCode Extensions: inject_dll_x86.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	SignalDesktop: Uninstall Signal.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	LogitechPresenter: Uninstaller.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	ChocoLatey: 7z.exe - HASH RULE	File Hash	
Allow	Everyone	VSCode Extensions: terraform-ls.exe - HASH RULE	File Hash	
Allow	Everyone	StreamDeck: twitchstudiotostreamdeck.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: winscp.exe - HASH RULE	File Hash	
Allow	Everyone	SignalDesktop: Signal.exe - HASH RULE for signed file	File Hash	

# Application whitelisting the easy way



# Application whitelisting the easy way

The screenshot shows a terminal window with a dark theme. The menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. The title bar shows the search term "AaronLocker". The left pane is an Explorer view showing a directory structure under "AARONLOCKER". The file "UnsafePathsToBuildRulesFor.ps1" is selected and highlighted with a blue background. The right pane displays the contents of this file.

```
UnsafePathsToBuildRulesFor.ps1
AaronLocker > CustomizationInputs > UnsafePathsToBuildRulesFor.ps1

75  @{
76    label = "OneDrive";
77    paths = "$env:LOCALAPPDATA\Microsoft\OneDrive";
78    pubruleGranularity = "pubProduct";
79  }
80
81  @{
82    label = "1Password";
83    paths = "C:\Users\patrick\AppData\Local\1Password\app\8";
84    pubruleGranularity = "pubOnly";
85  }
86
87  @{
88    label = "SignalMessenger";
89    paths = "C:\Users\patrick\AppData\Local\Programs\signal-desktop";
90    pubruleGranularity = "pubOnly";
91  }
92
93  @{
94    label = "AVDRemoteDesktop";
95    paths = "C:\Users\patrick\AppData\Local\Apps\Remote Desktop";
96    pubruleGranularity = "pubProduct";
97  }
```

# Application whitelisting the easy way

## Tips:

- Add your computer to domain if applicable
  - AaronLocker will scan UNC paths
- Add exception rules to the “CustomizationInputs” scripts
- Don’t add AppLocker rules manually
  - Do not exclude a complete user writeable folder, or you’re doomed!
- Rerun AaronLocker on updates (filehashes will change!)



Local Admin Password Protection

# Local Admin Password Protection

- Prevent identical local admin passwords on every session host
- Prevent pass the hash attacks
- Procedures for non-persistent images
  - CTX331247: Randomizing Local Admin Passwords in Non-persistent Environments



Block east-west network traffic

# Block east-west network traffic

Microsoft Azure

Search resources, services, and docs (G+ /)

Copilot

adm\_vandenborn@vand...  
VAN DEN BORN IT (VANDENBOR...)

Home > Virtual networks > PBO-VNET-MP

**PBO-VNET-MP | Subnets** Virtual network

Create Manage view ...

Filter for any field...

Name ↑

PBO-VNET-MP ...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Subnet Gateway subnet Refresh Manage users Delete

Search subnets

Name ↑	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	...
WVD-SN	10.100.1.0/24	-	250	-	-	-	...
GatewaySubnet	10.100.0.0/24	-	availability dependent ...	-	-	-	...

# Block east-west network traffic

Microsoft Azure Search resources, services, and docs (G+) Copilot 9 ? Export User

Home > Microsoft.NetworkSecurityGroup-20240923170556 | Overview >

## PBO-NSG-EASTWEST Network security group

Search Move Delete Refresh Give feedback JSON View

**Overview**

Resource group (move) : WVD-LABEU  
Location : West Europe  
Subscription (move) : Microsoft Partner Network  
Subscription ID : [REDACTED]  
Tags (edit) : Add tags

Custom security rules : 3 inbound, 3 outbound  
Associated with : 0 subnets, 0 network interfaces

**Inbound security rules**

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
100	Block-EastWest-Traffic-Inbound	Any	Any	10.100.1.0/24	Any	Deny
140	⚠ Deny-WinRM-Inbound	5986	TCP	Any	Any	Deny
150	Deny-RDP-Inbound	3389	Any	Any	Any	Deny
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

**Outbound security rules**

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
110	Block-EastWest-Traffic-Outbo...	Any	Any	Any	10.100.1.0/24	Deny
120	Deny-WinRM-Outbound	5986	TCP	Any	Any	Deny
130	Deny-RDP-Outbound	3389	Any	Any	Any	Deny
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65500	DenyAllOutbound	Any	Any	Any	Any	Deny

# Block east-west network traffic

Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authorized Computers	Authorized Local Principals	Local User Owner	PolicyAppld	Application Package
Block-EastWest-Traffic-Inbound	All	Yes	Block	No	Any	Any	10.100.1.0/24	Any	Any	Any	Any	Any	Any	Any	Any	None	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	TCP	9955	Any	Any	Any	Any	Any	None	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any	Any	Any	None	Any
App Installer	App Installer	Domain	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any	VANDENBORNI...	None	Microsoft.DesktopAp...
App Installer	App Installer	Domain	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any	XEL-W1123H2GM...	None	Microsoft.DesktopAp...
App Installer	App Installer	Domain	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	Any	XEL-W1123H2GM...	None	Microsoft.DesktopAp...
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any	Any	Any	Any	None	Any
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any	Any	Any	Any	Any	None	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any	Any	Any	Any	None	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	2177	Any	Any	Any	Any	Any	None	Any
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	2177	Any	Any	Any	Any	Any	None	Any

Actions

- New ...
- Filter ...
- Filter ...
- Filter ...
- View
- Refresh
- Export...
- Help
- Block-East

Windows Defender Firewall with Advanced Security

Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Computers	Authorized Local Principals	Local User Owner	PolicyAppld	Application Package	
Block-EastWest-Traffic-Outbound	All	Yes	Block	No	Any	Any	10.100.1.0/24	Any	Any	Any	Any	Any	Any	Any	None	Any	
AllJoyn Router (TCP-Out)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any	Any	Any	Any	None	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any	Any	Any	Any	Any	None	Any
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	XEL-W1123H2GM...	None	Microsoft.DesktopAp...	
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	XEL-W1123H2GM...	None	Microsoft.DesktopAp...	
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any	Any	Any	VANDENBORNI...	None	Microsoft.DesktopAp...	
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80	Any	Any	Any	Any	None	Any
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80, 443	Any	Any	Any	Any	None	Any
BranchCache Hosted Cache Server(HTT...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any	Any	Any	Any	Any	None	Any
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow	No	%System...	Any	Local subnet	UDP	Any	3702	Any	Any	Any	Any	None	Any

Actions

- New ...
- Filter ...
- Filter ...
- Filter ...
- View
- Refresh
- Export...
- Help



Block north-south network traffic

Block north-south traffic





Package manager

## Package manager



Adobe Acrobat (64-bit)

702 MB

11/28/2022

22.003.20282

Modify

Uninstall



Asian Language And Spelling Dictionaries Suppor...

182 MB

3/17/2022

22.003.20282 (Win), 22.003.20281 (Mac) Optional update, Nov 17, 2022

This release is a hotfix patch for Acrobat and Acrobat Reader that addresses some important bug fixes.

Package manager

WinGet



Evergreen



NeverRed

# Package manager

A screenshot of a web browser window displaying the Chocolatey Software | Packages page at <https://community.chocolatey.org/packages?q=adobe%20reader#package-warning>. The page features a purple header with a promotional message about livestream events. Below the header is a navigation bar with links for Main, Community, Docs, Blog, and Install. On the left, there's a sidebar for Software Authors listing authors like adobe, tracker software, claudio guarnieri, florian probst, gbooksdownloader.com, mariano graziano, and maxthon international limited, each with a count of packages (e.g., 3, 2, 1). The main content area shows search results for "adobe reader". A search bar at the top has the query "adobe reader" and a keyboard shortcut "ctrl k". Below the search bar, it says "Displaying Results 1 - 12". A button for "Manage Package Preferences" is visible. The central part of the page displays 12 stable community-maintained packages. The first package listed is "Adobe Acrobat Reader DC 2024.2.21005" with 546,298,083 downloads. It includes a thumbnail of the Adobe logo, a download button, and a command-line install link: > choco install adobereader. To the right, there's a green "Events" sidebar with a "View Events" button and a message about recent event additions.

Don't miss a byte of Chocolatey goodness! Explore our [livestream events now!](#)

Main Community Docs Blog Install

Learn Product Connect Sign In Sign Up

adobe reader ctrl k

Displaying Results 1 - 12 Manage Package Preferences

Found 12 Stable Community Maintained Packages searching for adobe reader

Software Authors

- adobe (3)
- tracker software (2)
- claudio guarnieri (1)
- florian probst (1)
- gbooksdownloader.com (1)
- mariano graziano (1)
- maxthon international limited (1)

Normal View Stable Only Relevance Reset Filters

**Community Package Repository Notification** Show Notification

**Adobe Acrobat Reader DC 2024.2.21005**  
546,298,083 Downloads  
View, print, sign, and annotate PDF files.  
By: Pauby  
Tags: adobereader adobe acrobat reader dc pdf mui multilanguage  
> choco install adobereader

Events

Find past and upcoming webinars, workshops, and conferences. New events have recently been added!

View Events

UNPACKING

# Package manager

```
Administrator: PowerShell  X + | - X
PowerShell 7.4.5
PS C:\Users\modok> choco upgrade all -y

3 validations performed. 2 success(es), 1 warning(s), and 0 error(s).

Validation Warnings:
- System Cache directory is not locked down to administrators.
  Remove the directory 'C:\ProgramData\ChocolateyHttpCache' to have
  Chocolatey CLI create it with the proper permissions.

Upgrading the following packages:
all
By upgrading, you accept licenses for the packages.
7zip v24.8.0 is the latest version available based on your source(s).
7zip.install v24.8.0 is the latest version available based on your source(s).
adobereader v2024.2.21005 is the latest version available based on your source(s).
az.powershell v12.2.0 is the latest version available based on your source(s).
azure-cli v2.63.0 is the latest version available based on your source(s).
```

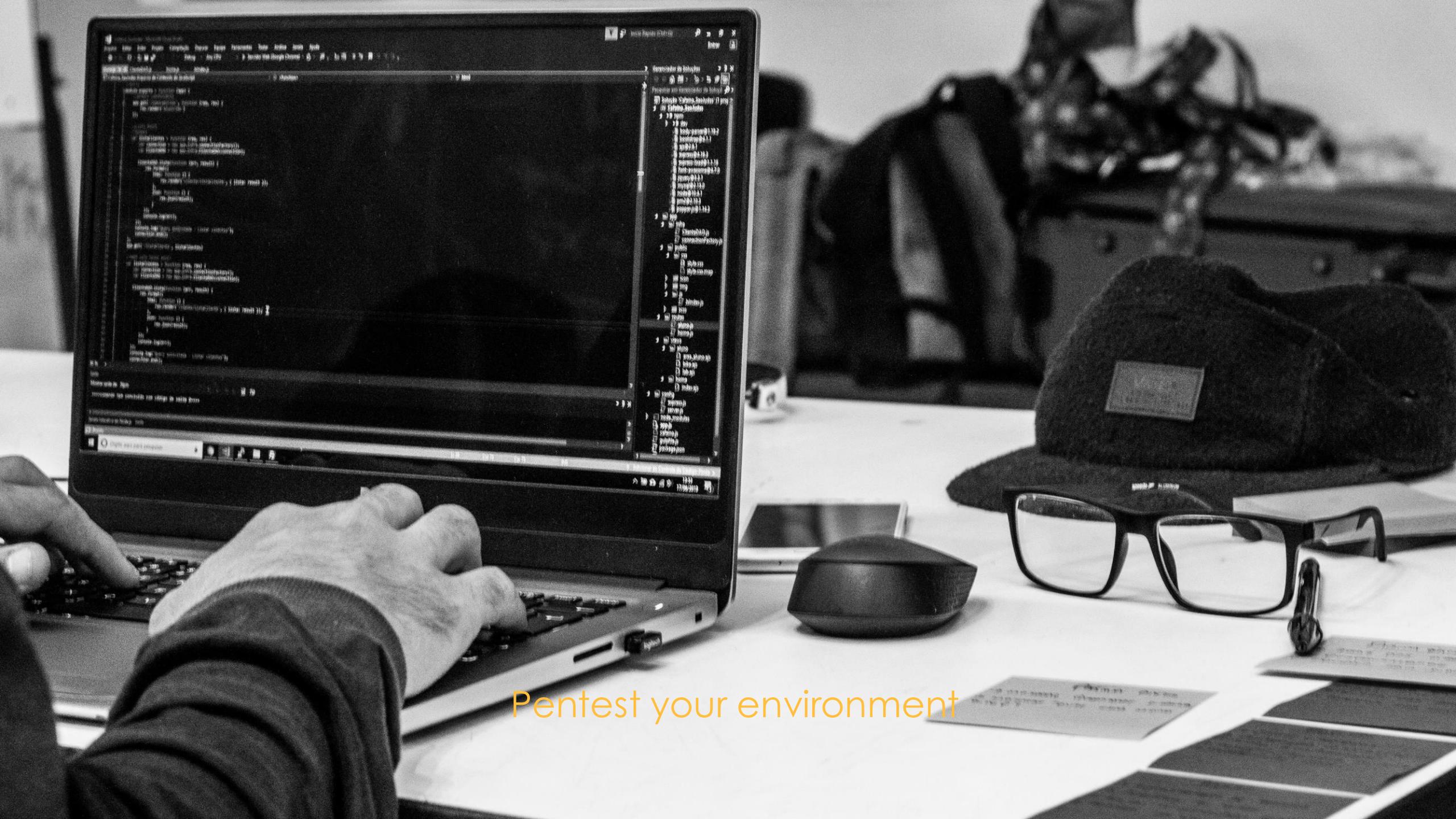
# Package manager

```
Administrator: PowerShell + - X

pdfsam v5.2.4 is the latest version available based on your source(s).
pdfsam.install v5.2.4 is the latest version available based on your source(s).

You have postman v11.7.0 installed. Version 11.10.0 is available based on your source(s).
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading postman 11.10.0... 100%

postman v11.10.0 [Approved]
postman package files upgrade completed. Performing other installation steps.
Downloading postman 64 bit
  from 'https://dl.pstmn.io/download/version/11.10.0/win64'
Progress: 100% - Completed download of C:\Users\modok\AppData\Local\Temp\chocolatey\postman\11.10.0\Postman-win64-11.10.0-Setup.exe (136.57 MB).
Download of Postman-win64-11.10.0-Setup.exe (136.57 MB) completed.
Hashes match.
Installing postman...
postman has been installed.
The upgrade of postman was successful.
Software installed as 'exe', install location is likely default.
PowerShell v5.1.14409.20180811 is the latest version available based on your source(s).
powershell-core v7.4.5 is the latest version available based on your source(s).
```



Pentest your environment

# Pentest your environment



Blue team



Red team



Regular



Fix findings



Wrap up

# Wrap up



Cyber war



Last line of defense



Harden golden image



CIS Policies



AaronLocker



East-West traffic  
North-South traffic



Package manager



Penetration test