

Hi this was my semi checklist kinda of a mess thing, I haven't updated this in ages tbh I really just used it as a easy way to get ot other docs if needed. At one point it was orginzed but yeah not anymore hope it helps tho

https://drive.google.com/file/d/1eE_nMPgiR9jpbkyJkXKLCpNm5YtZZm29/view?usp=sharing

Idk where to put this but, proc dump bad and good, its a cmd tool thats helpful but c an be used to dump lass.exe which is very no bueno, I believe the ASR rules fix this but just in case if ever seen on an image consider thanos snapping for points :)

















https://defsec.club/doku.php?id=ccdc_checklist
[ccdc_checklist \[DSU Computer Clubs Wiki\]](#)




<https://regexr.com>

<https://github.com/frizb/PasswordDecrypts>

Command list ig Authorized Administrators:ri o (you)password: 1L0vemoV13\$pr ofessor password: M4st3rM1nD!be rlin password: wallpalermo password: lI0v3B&rliNlisbo n password: 1nsp3cT0r! Authorized Users: Clkasjdf824DDD kjkid // password for windows box	Lusrmgr.msc dsa.msc for AD servers Secpol.msc gpupdate /force Fsmgmt.msc msconfig rd /s c:\\$Recycle.Bin rd/sc:\\$Recycle.Bin Gpedit.msc netstat -ab netstat -anbo netstat -ano Dnsmgmt.msc Command to find unquoted services - cmd /c wmic service get name,displayname,pathname,startmode findstr /i "auto" findstr /i /v "c:\windows\\" findstr /i /v "" ldaps Add-WindowsFeature Adcs-Cert-Authority - IncludeManagement Tools Install-AdcsCertificationAuthority -CAType EnterpriseRootCA MpAup.dll is bad delete it Local user powershell stuff Net user
--	---



	<p>PowerShell User Stuff</p> <ul style="list-style-type: none"> - “Get-Localuser” <ul style="list-style-type: none"> - Lists all local users - “Remove-Localuser” + name - Set-LocalUser (name) -PasswordNeverExpires \$False -UserMayChangePassword \$True - “Get-LocalGroup” - Remove-LocalGroup <Name> - get- <Name of group> - Add -localGroupMember <name of group> “<name of user>” <ul style="list-style-type: none"> - Include quotes on user - Remove -localGroupMember <name of group> “<name of user>” - Get-Childitem -Path C:\ -Recurse -Include "what you want to find (use * as a wildcard, e.g. *.txt, *.exe, etc) - Get-Childitem -Path C:\ -Recurse -Directory "directory u want to find" - Import-Module .\Invoke-HardeningKitty.ps1 - lu / Set-ExecutionPolicy Restricted - Invoke-HardeningKitty -Mode HailMary -Log -Report -FileFindingList .\lists\finding_list_0x6d69636b_machine.csv <p>PSEXEC</p> <ul style="list-style-type: none"> - psexec -accepteula -i -s cmd.exe <ul style="list-style-type: none"> - Run system as NT Authority User (Highest perms possible) - Check if it worked with “whoami” in new cmd - Output should be nt authority\system
--	--

Key Doc Links	<ul style="list-style-type: none">  Server Checklist  user rights assignment  Security Options  Services  DLL injections  Scheduled Task/Job  BackDoor Research  Windows CyberSpace Tool List  firefox-hardening-checklist C:\Windows\System32\GroupPolicy  Active directory / DNS  Harden Kitty solo commands  IIS Server Last Year's Cyber Slides Yes COPE  Random resource doc ig  Doc of registry  WMI Persistence  Open SSH
---------------	---

	<ul style="list-style-type: none">  MySQL security  Mushroom Kingdom Server - Image Guide.pdf  Previous Vulns List  Copy of KAC Image Walkthrough <p> https://www.ired.team/offensive-security/privilege-escalation https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite https://learn.microsoft.com/en-us/sysinternals/downloads/psexec https://www.nirsoft.net/utils/advanced_run.html https://www.blackviper.com/service-configurations/ https://www.virustotal.com/gui/home/url Op virus total truly giga chad </p>
--	--

Control panel	Turn On
Firewall	Search name and click turn on (note that gpedit has a more advanced version of this)
UAC	Put slider to max
Control panel	Turn Off
Remote settings	Turn off both remote assistance and remote desktop
Autoplay	Search auto play and disable / also can go to hardware and sounds
Programs and Features (appwiz.cpl)	Turn On
Anything in read me	Appwiz.cpl > left bar has features> click the button to enable
Powershell 2.0	Appwiz.cpl > left bar has features> click the button to enable
.NET Framework	Appwiz.cpl > left bar has features> click the button to enable
Programs and Features (appwiz.cpl)	Turn Off (https://www.bcuninstaller.com) use this for killing useless stuff
Telnet client ass 10	Appwiz.cpl > left bar has features> unclick the button to enable
SMB 1	Appwiz.cpl > left bar has features> unclick the button to enable
Remote desktop	Appwiz.cpl > left bar has features> unclick the button to enable `
Anything in read me	Appwiz.cpl > left bar has features> unclick the button to enable

File Explorer Options	
Hidden files	Turn on in options
Ultra search	Use ultra search to find any files than need to be removed
Local user management	Lusrmgr.msc / dsa.msc for AD servers
Disable	
Default guest	Disable Rename Password expires User cannot change password
Default Administrator	Disable Rename the Administrator Account Password expires User cannot change password
Users	Check read me for who to add/who to remove <ul style="list-style-type: none"> - Change all passwords - Password expires -
built-in accounts / general group or accounts	<ul style="list-style-type: none"> - Make sure that accounts only have access to necessary privs - Check each group privileges to make sure there is no abuse of power in the system
Groups	Check read me for who to add/who to remove <ul style="list-style-type: none"> - Only guest should be in the guest group - Unless specified there should be NO ONE in the Remote Desktop Users group
GPEDIT	https://drive.google.com/drive/folders/1mT_ngxsXeyhKxGl8466nBdXEc5F7Z8kM?usp=share_link
Local Security Policy	Secpol.msc ./ gpupdate /force
Password Policies	Enforce password history: 10 Maximum password age: 90 Minimum password age: 30 Minimum password length: 14 Password must meet complexity requirements: Enabled

Windows Defender Windows Event Log	
Shares	fsmgmt.msc
Default shares	ADMIN\$ C\$ IPC\$ Perms for non default shares that are allowed on the home system <ul style="list-style-type: none"> - Everyone should not have any access - Normal users read only - Admins full <ul style="list-style-type: none"> - Or read and write
Internet Explorer	Click on Gear icon
Security tab	Set all the highest except for trusted site which can be medium
SMB security enhancements	Enable SMB Encryption with Windows PowerShell <ul style="list-style-type: none"> - Set-SmbServerConfiguration –EncryptData \$true - New-SmbShare –Name <sharename> -Path <pathname> –EncryptData \$true Block inbound SMB access Block TCP port 445 inbound from the internet at your corporate hardware firewalls. Blocking inbound SMB traffic protects devices inside your network by preventing access from the internet. Disable SMB Server if unused <ul style="list-style-type: none"> -
Privacy tab	Cookies set to second highest, or to accept first-party and block third-party Pop-up blocker
DDL Injections	 DLL injections
Scheduled Task/Job	 Scheduled Task/Job
Windows Defender Security Center -> App & browser control -> Exploit protection settings -> System settings	Make sure <ul style="list-style-type: none"> - Everything is turned on and all exceptions are known to be safe
Random Crap	Removed phpinfo file PHP display errors has been disabled IIS server requires use of SSL connections



ASR rule implementation (should already be done can check if you want)	https://github.com/anthonws/MDATP_PoSh_Scripts
Windows Firewall Checklist	https://www.sans.org/media/score/checklists/FirewallChecklist.pdf
ntds.dit	C:\Windows\NTDS C:\Windows\System32\ C:\Windows\WinSxS\amd64_microsoft-windows-d..rvices-domain-f iles_31bf3856ad364e35_10.0.17763.1_none_8bd0f81f9b897a08
Alternative data streams	https://learn.microsoft.com/en-us/sysinternals/downloads/streams

Persistence	
Clean all recycle bins	rd /s c:\$Recycle.Bin
Task Scheduler	<ul style="list-style-type: none"> - If anything is being repeated check task scheduler - Restart system after turning off - Make sure to show hidden tasks - Look at the name, the trigger, and the action upon trigger of each active task
IEDK	Make sure C:\inetpub\wwwroot doesn't have a shell.php in it
GPEDIT	Gpedit.msc
Registry being cringe	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Also check HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ->Anything in here would execute whenever a specific user logged in
Event logs	Tool used to view events logs
To find type of event	Use the event IDs
Backdoors	Go to cmd and use netstat -anbo - TestFor-StickyKey

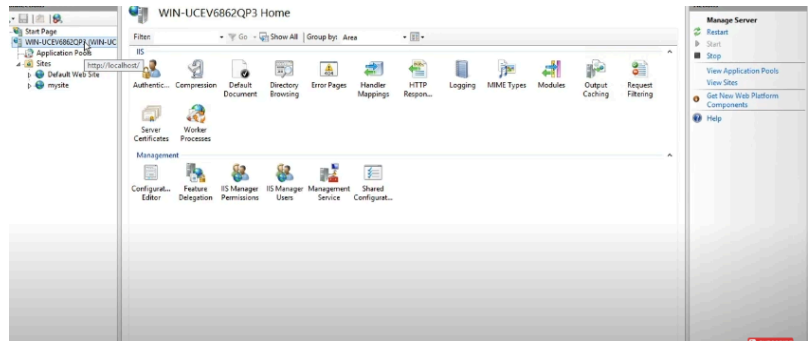
	<ul style="list-style-type: none"> - Check for sticky key back doors /turn off sticky keys <div>BackDoor Research</div> <pre>taskkill /PID <PID> /F del C:\Windows\system32\sethc.exe</pre> <p>Sends shift 5 times using xdotool to trigger sethc.exe backdoors Sends Windows+u using xdotool to trigger utilman.exe backdoors</p> <p>sethc.exe/utilman.exe can be back doors to figure out if they are back doors check if they where editing or if using them opens smth else up</p>
To kill a connection 5900/49664	<ol style="list-style-type: none"> 1) netstat -ano findstr :<PORT> 2) taskkill /PID <PID> /Fg 3) anbo <div>C:\WINDOWS\system32>netstat -ano findstr :8080</div> <pre>TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING TCP [::]:8080 [::]:0 LISTENING</pre> <p>The area circled in red shows the PID (process identifier). Locate the PID of the process the port you want.</p> <p>Step 2:</p> <p>Next, run the following command:</p> <div>taskkill /PID <PID> /F</div> <p>(No colon this time)</p> <div>C:\WINDOWS\system32>taskkill /PID 3740 /F</div> <pre>SUCCESS: The process with PID 3740 has been terminated.</pre> <ol style="list-style-type: none"> 4)
Computer name	<p>Change description</p> <p>Change network ID</p> <ul style="list-style-type: none"> - Joining workgroup/domain <p>Change computer name/domainS</p>
5.1 System Properties	<p>Computer Name</p> <ul style="list-style-type: none"> - Change the name of the pc / change network ID <ul style="list-style-type: none"> - Joining workgroup / domain - Change computer name / domain <p>Hardware</p> <ul style="list-style-type: none"> - Basically the only important thing here is DEP <ul style="list-style-type: none"> - Performs additional checks on memory to prevent malicious code from running - Should turn on for ALL
Advanced	<ul style="list-style-type: none"> - msconfig <ul style="list-style-type: none"> - The System Configuration utility - Boot <ul style="list-style-type: none"> - Turn on safe boot and everything else that is useful <ul style="list-style-type: none"> - Alternate shell

	<ul style="list-style-type: none"> - Boots into a command prompt without GUI or networking - Do not do this unless pain is wanted - Summary <ul style="list-style-type: none"> - The main things you will want to look at in msconfig are the non-Microsoft services and the startups. You can also check out the shortcut tools provided by it. -
System Protection	Set up restore point in case of failure
Remote	No remote assistance Remote Desktop disabled
5.2 System Configuration Utility	Run > msconfig General <ul style="list-style-type: none"> - Normal - Diagnostic <ul style="list-style-type: none"> - Only basic drivers and services start - Selective <ul style="list-style-type: none"> - Choose what loads - Boot <ul style="list-style-type: none"> - Control/modify Windows boot environment - Safe boot includes many options - Only really useful for boot troubleshooting - Services <ul style="list-style-type: none"> - Select which services are started at boot - Most useful thing is “Hide all Microsoft services” <ul style="list-style-type: none"> - Shows you custom services - Type of monitors <ul style="list-style-type: none"> - Reliability Monitor - Resources monitors - Task monitor
General	<ul style="list-style-type: none"> ◦ Normal ◦ Diagnostic <ul style="list-style-type: none"> ◦ Only basic drivers and services start ◦ Selective <ul style="list-style-type: none"> ◦ Choose what loads
Boot	Ignore outside of troubleshooting
Services	<ul style="list-style-type: none"> - Hide all microsoft services - Select which services are started at boot

Startup	<ul style="list-style-type: none"> - Make sure nothing bad is running at startup
Tools	CyberPat Tools List
Performance monitor	Counter - specific measurement for objects Counters exist for cache, memory, paging file, disk, etc.
Windows Registry	Doc of registry
Advanced sharing settings	<ul style="list-style-type: none"> - Turn on file printer sharing - Turn on password
WMI persistence	<p>https://www.makeuseof.com/windows-wmi-persistence-removal/</p> <p>WMI persistence refers to an attacker installing a script, specifically an event listener, that is always triggered when a WMI event happens. For instance, this will occur when the system boots or the system administrator does something on the PC, like opening a folder or using a program.</p> <p>Persistence attacks are dangerous because they are stealthy. As explained on Microsoft Scripting, the attacker creates a permanent WMI event subscription that executes a payload that works as a system process and cleans up logs of its execution; the technical equivalent of an artful dodger. With this attack vector, the attacker can avoid getting discovered through command-line auditing.</p> <p>Use Autoruns</p> <p>https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns</p>
VMware networking	NAT <ul style="list-style-type: none"> • share IP with host • has internet • best option for general use Host-only <ul style="list-style-type: none"> • VM gets own private address • cannot talk to host • no internet unless specific settings are defined

	<ul style="list-style-type: none"> • can talk to other host-only set VMs • best option for networking two VMs on the same computer <p>Bridged</p> <ul style="list-style-type: none"> • VM is like another computer in the network that the host is in • has internet if settings are right • best option for networking two VMs in the same network
Firefox	 firefox-hardening-checklist
Windows registry	<p>There is a lot on here :</p> <p>https://docs.google.com/presentation/d/1dWLiXJsciiEQMay244QRgdC9K0phM0piqyPoew7PB9s/edit?usp=sharing</p>
Active directory / DNS server	 Active directory / DNS
Wordpress	<ul style="list-style-type: none"> - Should be found at localhost/wordpress/wp-admin <ul style="list-style-type: none"> - Need to login with proper credentials - what to do <ul style="list-style-type: none"> - update wordpress - manage users - check media - manage plugins (update, remove unnecessary ones) - manage pages, comments, a bunch of other minor stuff - Disable File Editing <ul style="list-style-type: none"> - This can be turned off in the wp-config.php file with the command - define('DISALLOW_FILE_EDIT', true) - if you see a similar line already in the file, change it otherwise, just add this line in and save the file - Limit Login Attempts <ul style="list-style-type: none"> - To prevent this you can install and activate the Login LockDown plugin. - Disable Directory Indexing and Browsing <ul style="list-style-type: none"> - Locate the .htaccess file in your website's root directory and add the line: <ul style="list-style-type: none"> - Options -Indexes - Automatically Log Out Idle Users <ul style="list-style-type: none"> - To prevent this install and activate the Inactive Logout plugin. <p>How to setup a wordpress server</p> <p>Download and instal IIS</p> <p>Right click on the "Sites" folder thing</p> <p>Go to add website</p>

Go to wwwroot for the physical directory; now make a new folder that is the same name as the site name.
 Set up https with a self signed SSL cert
 Now got to the folder you just made and create an index.html to test
 To get wordpress going you want to go back to the top of the IIS server stuff



Click on get new web platform components
 Install the necessary data
 Click on the new web platform again
 Search word press again and install
 In configure or install make sure to pick the site you want to add this on

CRAZY ASS VUNS

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/vssadmin-delete-shadows>

vssadmin list shadows

Connection status: OK

Internet Connectivity Check: N/A
 Aeacus Server Connection Status: N/A

0 penalties assessed, for a loss of 0 points:

10 out of 61 scored security issues fixed, for a gain of 17 points:

Removed unauthorized Schema admin Alan - 1 pts
 Removed unauthorized DNS admin Bitzi - 1 pts
 Authenticated users cannot add workstations to the domain - 1 pts
 Domain users cannot enable computer and user accounts to be trusted for delegation - 1 pts
 Powershell 2.0 has been uninstalled - 1 pts
 WinDivert user-mode driver has been removed, how tf did u get this? DM me - 4 pts
 Alternate data stream with PII removed - 1 pts
 Volume shadow copy with insecure SAM permissions deleted - 4 pts
 LDAP anonymous access has been disabled - 2 pts
 DNS zone lakewood.com is signed - 1 pts

The Aeacus project is free and open source software. This project is in no way endorsed or affiliated with the Air F

WinDivert is a user-mode packet capture-and-divert utility for Windows. It allows for capturing and modifying network packets at the network layer, and can be used for a wide range of tasks such as network traffic analysis, packet filtering, and network security. WinDivert is a user-mode library that runs in user-space and does not require any kernel-mode drivers or special privileges. This allows for easy deployment and eliminates the need for administrative

	<p>rights or signing drivers.</p> <p>WinDivert uses a powerful and flexible filtering language similar to the popular libpcap library, and can capture and divert packets from all network layers, including raw IP packets. It also provides a set of API to create, modify, and inject packets on the fly.</p> <p>WinDivert is a powerful tool, but it requires a certain level of expertise to use and understand. It can be used for a number of purposes like network analysis, packet filtering, network security, and more. It is not recommended to use it without proper knowledge of how it works, as it may cause serious issues to your system.</p> <p>WMI persistence removed</p> <ul style="list-style-type: none"> ○ Can be found in Autoruns <ul style="list-style-type: none"> ■ Autoruns only removes 1 of the 3 components. <ul style="list-style-type: none"> ● Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter "Name='Twitter'" Remove-WmiObject -Verbose ● Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter "Name='Twitter'" Remove-WmiObject -Verbose ● Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter "__Path LIKE '%Twitter%'" Remove-WmiObject -Verbose <p>Or</p> <p>Set-Service -Status Stopped -StartupType Disabled -Name Winmgmt</p> <ul style="list-style-type: none"> ● Default powershell script double click behavior not set to execute <ul style="list-style-type: none"> ○ HKEY_CLASSES_ROOT\Microsoft.PowerShellScript.1\Shell\{Default} not set to 0 ○ Other valid options are Open and Edit which will spawn a notepad or ISE window with the given script
--	--

User Right in Group Policy	Name of Constant
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege

Access this computer from the network	SeNetworkLogonRight
Act as part of the operating system	SeTcbPrivilege
Add workstations to domain	sSeMachineAccountPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight
Allow log on through Terminal Services	SeRemoteInteractiveLogonRight
Back up files and directories	SeBackupPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Change the system time	SeSystemtimePrivilege
Change the time zone	SeTimeZonePrivilege
Create a pagefile	SeCreatePagefilePrivilege
Create a token object	SeCreateTokenPrivilege
Create global objects	SeCreateGlobalPrivilege
Create permanent shared objects	SeCreatePermanentPrivilege
Create symbolic links	SeCreateSymbolicLinkPrivilege
Debug programs	SeDebugPrivilege
Deny access to this computer from the network	SeDenyNetworkLogonRight
Deny log on as a batch job	SeDenyBatchLogonRight
Deny log on as a service	SeDenyServiceLogonRight
Deny log on locally	SeDenyInteractiveLogonRight
Deny log on through Terminal Services	SeDenyRemoteInteractiveLogonRight
Enable computer and user accounts to be trusted for delegation	SeEnableDelegationPrivilege
Force shutdown from a remote system	SeRemoteShutdownPrivilege
Generate security audits	SeAuditPrivilege
Impersonate a client after authentication	SeImpersonatePrivilege
Increase a process working set	SeIncreaseWorkingSetPrivilege

Increase scheduling priority	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	SeLoadDriverPrivilege
lock pages in memory	SeLockMemoryPrivilege
Log on as a batch job	SeBatchLogonRight
Log on as a service	SeServiceLogonRight
Manage auditing and security log	SeSecurityPrivilege
Modify an object label	SeRelabelPrivilege
Modify firmware environment values	SeSystemEnvironmentPrivilege
Perform volume maintenance tasks	SeManageVolumePrivilege
Profile single process	SeProfileSingleProcessPrivilege
Profile system performance	SeSystemProfilePrivilege
Remove computer from docking station	SeUndockPrivilege
Replace a process level token	SeAssignPrimaryTokenPrivilege
Restore files and directories	SeRestorePrivilege
Shut down the system	SeShutdownPrivilege
Synchronize directory service data	SeSyncAgentPrivilege
Take ownership of files or other objects	SeTakeOwnershipPrivilege

How to Encrypt files on Windows:

- Step 1. Select one or more files or folders.
- Step 2. Right-click the selected data >Properties.
- Step 3. Click Advanced...
- Step 4. Select the Encrypt contents to secure data check box.
- Step 5. Files and folders that have been encrypted with EFS are displayed in green, as shown in the figure.

Resources for Forensics Qs

- steg (images, audio files, etc)
 - image - aperisolve.fr
 - image - <https://stegonline.georgeom.net/>
 - audio - <https://databorder.com/transfer/morse-sound-receiver/>

- corrupted files - hexed.it
- Rishabh (all in one package lol)
- crypto
 - best one; has ciphers, encryption schemes, etc - <https://gchq.github.io/CyberChef/>
 - hashes - <https://hashes.com/en/decrypt/hash>
 - ciphers - <https://rumkin.com/tools/cipher/>
 - bip39 mnemonic seed
 - <https://particl.github.io/bip39/bip39-standalone.html>
 - <https://learnmeabitcoin.com/technical/mnemonic>
 - random ciphers ig? - <http://quipqiup.com/>
 - Rishabh (all in one package lol)

☰ Rd1 Windows Log

☰ CIS

☰ Round X

☰ Windows round 2 log

v3Rysecurep@sSworD

&rpDzPo9tnz43

BR7D-URCS-9KV4

Set-ExecutionPolicy Unrestricted / Set-ExecutionPolicy Restricted

Mario:S3cure%The%Shr00ms / MushroomMan64

Rudolph:R3indeerSl@ys

stubblefield (you)

Password: v3Rysecurep@sSworD

lusrmgr.msc

<https://support.kaspersky.com/5350> (rootkit scanner always run this !)

<https://www.roguesecurity.in/2018/12/02/a-guide-for-windows-penetration-testing/>

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

<https://github.com/rasta-mouse/Sherlock/blob/master/Sherlock.ps1>

<https://github.com/AonCyberLabs/Windows-Exploit-Suggester>

<https://github.com/PowerShellMafia/PowerSploit>

<https://www.metasploit.com/download>

https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.ht

[ml](#) - for forensics with CVE stuff

<https://cyberlab.com/> - PCcleaner

<https://www.microsoft.com/en-us/download/details.aspx?id=9905>