Windows 10 Checklist

By Lakshay Kansal

Script (this is only relevant if you have made a script)

To run the scripts download the Windows 10 folder to the desktop then cd in the folder and run these commands.

```
Set-ExecutionPolicy -Scope LocalMachine -ExecutionPolicy Unrestricted
-Force

./start.ps1
```

Forensic Questions

Just answer them… to the best of your ability. Should be simple for rounds 1 and 2. Google is your friend.

Net Stuff

Shared Drives

```
net share
```

Connected Remote Session

```
net session

net session \\computername /del
```

User Management

Control Panel -> User Accounts -> Manage User Accounts

- Delete Users that are not in the readme.
- Add Users that are in the readme but not in the user list.
- Make Users that are supposed to be administrators (according to the readme) administrators.
- Make Users that are not supposed to be administrators but are administrators, normal users.
- Change the Passwords of Users that are insecure to a secure password. (eg. !amAw3s0m3)

Password Policies

Win + R -> type “secpol.msc” -> Account Policies -> Password Policy

- Enforce Password History = 5
- Maximum Password Age = 90
- Minimum Password Age = 30
- Minimum Password Length = 8-10
- Password Must Meet Complexity Requirements = enabled
- Store Password Using Reversible Encryption for All Users = disabled

Win + R -> type “secpol.msc” -> Account Policies -> Account Lockout Policy

- Account Lockout Duration = 30 min
- Account Lockout Threshold = 5
- Reset Account Lockout Counter After = 30 min

Local Policies

Win + R -> type “secpol.msc” -> Local Policies -> Audit Policy

- Make everything success and failure
- If you lose points you can turn it back

Win + R -> type “secpol.msc” -> Local Policies -> User Rights Assignment

- Access this computer from the network = only administrator

Win + R -> type “secpol.msc” -> Local Policies -> Security Options

- Interactive logon: Do not require CTRL + ALT + DEL = disabled
-

Updates

- Update Firefox (probably gonna have to do it 3 times because it doesn’t update fully in one go)
- Update Applications that they say are necessary in the readme (eg. Notepad++)
- Update Windows 10 (it takes a long time but it is worth it in the end)

Firefox

- Go to Settings
- Make sure Firefox Blocks Dangerous Downloads
-

Applications

- Delete sus applications (unless the readme says otherwise)
    - Npcap
    - Wireshark
    - Keyloggers
    - John

Sharing Drives

- Don’t share drives. That means anyone can see the things inside. Here is how you turn it off.

File Explorer -> This PC -> Right Click Local Disk -> Share With -> Advanced Sharing -> Uncheck Share this Folder

Backups

Set up a backup
Control Panel -> System and Security -> Backup and restore

Event Viewer

Check for sketchy stuff in the audit logs.

- Application: events logged by programs
- Security: any successful or unsuccessful login attempts

- Setup: Events that occurred during installation
- System: Events logged by system components
- Forwarded Events: Events forwarded from other computers

Internet Options

Advanced Tab:

Privileges

Who has access to drives and things.

Windows Features

Control Panel -> Programs -> Programs and Features -> Turn Windows Features on or off

- SMB
- FTP
- Telnet
- Internet Explorer 11
- Legacy Components - Direct Play
- Media Features - Windows Media Player
- Microsoft Print to PDF
- Internet Printing Client
- Windows Fax and Scan
- Remote Differential Compression API Support
- Windows Powershell 2.0
- Windows Process Activation Service (Internet Information Services)
- Work Folders Client
- XPS Services and Viewer

Settings

- Potentially Unwanted App (Settings -> Update & Security -> Windows Security -> App & Browser Control) Set to warn or block.
- Exploit protection (Settings -> Update & Security -> Windows Security -> App & Browser Control) Turn everything on.

- Core Isolation / Memory Integrity (Settings -> Update & Security -> Windows Security -> Device Security) Turn it on.
- Controlled Folder Access (Settings -> Update & Security -> Windows Security -> Virus & Threat Protection) Turn it on. Add protected folders.
- Turn off ads and tracking (Settings -> Privacy -> General -> Change Privacy Options) Make it off, on, off, off.
- Diagnostics data (Settings -> Privacy -> Diagnostics & Feedback) Set it to full.
- (Settings -> Privacy -> Location) Disable stuff like location, microphone, camera, if needed/desperate.
- Turn AutoPlay off. (Settings -> Devices -> AutoPlay)
- Bluetooth Security (Settings -> Devices -> Bluetooth & Other Devices -> More Bluetooth Options) Turn off “Allow Bluetooth devices to find this PC”
- Disable Automatic Login

Network Scanning

Go to Powershell (Remember to Run as Admin)

```
Set-MpPreference -DisableScanningNetworkFiles 0
```

This enables Windows Defender to scan network files. If you want to turn it off, replace the 0 with a 1.

Port Checks

Go to Command Prompt

```
netstat -ab
```

```
netstat -aon

netstat -ano -p tcp 5
```

Listening status means the port is open.
You can check which port is connected to which service through the PID of the port and the service.

Windows Firewall

- Control Panel -> System and Security -> Windows Firewall->Change notification settings
- Turn Firewall on for Home, Work, and Public
- Select “Block all incoming connections, including those in the list of allowed programs” for both
- Select “Notify me when Windows Firewall blocks a new program” for both
- Control Panel -> System and Security -> Windows Firewall->Advanced settings
- Allow trusted programs to connect without being blocked by adding them to your Windows Firewall

Exceptions list

- For each network type, you can customize whether you want the programs allowed through

It’s much safer to allow only certain programs through your firewall than to open an entire port to traffic

- Ports are numbers that identifies one side of a connection between two computers

Common Exceptions

- Core Networking
  - Regular Microsoft Windows services that retrieve data from the Internet
  - If you don’t enable this exception across all three types of networks, some Microsoft services and programs will not run properly
- File and Printer Sharing - off
- Remote Assistance - off
- Remote Desktop - off
- UPnP Framework (Universal Plug-and-Play) -off

Advanced Settings

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Windows Defender

Local Group Policy Editor -> Computer Configuration -> Administrative Templates -> Windows Components -> Windows Defender Antivirus

- MAPS

    - Join Microsoft MAPS, Enabled Advanced MAPS
    - Block at First Sight, Enabled
- MpEngine
    - Configure extended cloud check, Enabled 20 seconds
    - Select cloud protection level, High+ level enabled

Go to Powershell

```
Set-MpPreference -PUAProtection 1
```

Rootkit

If you are stuck I guess you could go ahead and do some rootkit detection using the free malwarebytes tool.

Ton of Policies and Registry Keys

```
MinimumPasswordAge = 5

MaximumPasswordAge = 60

MinimumPasswordLength = 12

PasswordComplexity = 1

PasswordHistorySize = 24

LockoutBadCount = 10

ResetLockoutCount = 20

LockoutDuration = 20

ForceLogoffWhenHourExpire = 1
```

```
NewAdministratorName = "modlevel"
NewGuestName = "bignoob"
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableAdminAccount = 0
EnableGuestAccount = 0
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 3
AuditDSAccess = 3
AuditAccountLogon = 3
[Privilege Rights]
SeTrustedCredManAccessPrivilege =
SeNetworkLogonRight = *S-1-5-32-555,*S-1-5-32-544
SeTcbPrivilege =
SeIncreaseQuotaPrivilege = *S-1-5-20,*S-1-5-19,*S-1-5-32-544
SeInteractiveLogonRight = *S-1-5-32-545,*S-1-5-32-544
```

```
SeRemoteInteractiveLogonRight = *S-1-5-32-555,*S-1-5-32-544

SeBackupPrivilege = *S-1-5-32-544

SeSystemtimePrivilege = *S-1-5-19,*S-1-5-32-544

SeTimeZonePrivilege = *S-1-5-32-545,*S-1-5-19,*S-1-5-32-544

SeCreateTokenPrivilege =

SeCreateGlobalPrivilege = *S-1-5-6,*S-1-5-20,*S-1-5-19,*S-1-5-32-544

SeCreatePermanentPrivilege =

SeCreateSymbolicLinkPrivilege = NT VIRTUAL MACHINE\Virtual Machines,*S-1-5-32-544

SeDebugPrivilege = *S-1-5-32-544

SeDenyNetworkLogonRight = *S-1-5-113,*S-1-5-32-546

SeDenyBatchLogonRight = *S-1-5-32-546

SeDenyServiceLogonRight = *S-1-5-32-546

SeDenyInteractiveLogonRight = *S-1-5-32-546

SeDenyRemoteInteractiveLogonRight = *S-1-5-113,*S-1-5-32-546

SeEnableDelegationPrivilege =

SeRemoteShutdownPrivilege = *S-1-5-32-544

SeAuditPrivilege = *S-1-5-20,*S-1-5-19

SeImpersonatePrivilege = *S-1-5-6,*S-1-5-20,*S-1-5-19,*S-1-5-32-544

SeIncreaseBasePriorityPrivilege = *S-1-5-32-544

SeLoadDriverPrivilege = *S-1-5-32-544

SeLockMemoryPrivilege =

SeBatchLogonRight = *S-1-5-32-544
```

```
SeServiceLogonRight =

SeSecurityPrivilege = *S-1-5-32-544

SeRelabelPrivilege =

SeSystemEnvironmentPrivilege = *S-1-5-32-544

SeManageVolumePrivilege = *S-1-5-32-544

SeProfileSingleProcessPrivilege = *S-1-5-32-544

SeSystemProfilePrivilege = *S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420,*S-1-5-32-544

SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19

SeRestorePrivilege = *S-1-5-32-544

SeShutdownPrivilege = *S-1-5-32-545,*S-1-5-32-544

SeTakeOwnershipPrivilege = *S-1-5-32-544

[Registry Values]

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,"1"

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"2"

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,"1"

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"4"

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,10

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin=4,2

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser=4,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
```

```
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserNam
e=4,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLockedUserI
d=4,3

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetecti
on=4,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA=4,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths=4
,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableUIADesktopToggle
=4,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization=4
,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorTok
en=4,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs=
4,900

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\Su
pportedEncryptionTypes=4,2147483640

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"
ORANGE MAN BAD"

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,No
Hack PLS

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\MaxDevicePasswordFaile
dAttempts=4,10

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnectedUser=4,3

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop=
4,1

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4
,0
```

```
MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\allownullsessionfallback=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395200

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395200

MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\pku2u\AllowOnlineID=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\UseMachineId=4,1

MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Mach
ine=7,System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\S
erver Applications,Software\Microsoft\Windows NT\CurrentVersion

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine=7
,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows
NT\CurrentVersion\Windows,System\CurrentControlSet\Control\Print\Printers,System\Current
ControlSet\Services\Eventlog,Software\Microsoft\OLAP
Server,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Te
```

```
rminal Server,System\CurrentControlSet\Control\Terminal
Server\UserConfig,System\CurrentControlSet\Control\Terminal
Server\DefaultUserConfiguration,Software\Microsoft\Windows
NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog

MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=4,1

MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignatur
e=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignatu
re=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess
=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\SmbServerNameHardening
Level=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPa
ssword=4,0

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySig
nature=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySi
gnature=4,1

MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,25

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
```

```
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
```