# Windows Security

This document is used as a checklist and guideline to Windows hardening. I will try to explain the best I can what each thing does. Also, this document will be formatted from a general to more OS specific list. Some things may be different in the many OS’s like Computer/THIS PC

## General Windows Security

### Users and Groups

**Delete any unnecessary users.**

Start > Right click Computer > Manage > Local Users and Groups > Users

**Add/Remove users from any inappropriate groups.**

Start > Right click Computer > Manage > Local Users and Groups > Groups

**Lock any inactive users.**

Start > Right click Computer > Manage > Local Users and Groups > Users > Right click > Properties > Check Account is Disabled

**Change password of a user.**

Start > Right click Computer > Manage > Local Users and Groups > Users > Right click > Set Password

**Create a user**

Start > Right click Computer > Manage > Local Users and Groups > Users > Right click open space > New User

**Rename the guest account**

Start > secpol.msc > Local Policies > Security Options > Accounts: Rename guest account

**Disable the guest account**

Start > secpol.msc > Local Policies > Security Options > Accounts: Guest account status

**Rename the Administrator account**

Start > secpol.msc > Local Policies > Security Options > Accounts: Rename administrator account

**Disable the Administrator account**

Start > secpol.msc > Local Policies > Security Options > Accounts: Administrator account status

**FIX YOUR TIME SERVER**

**Check the host file**

Start>C:>Windows>System32>drivers>etc>hosts> open with Notepad

Delete Share from command prompt  
**net share *sharename /delete***

Change the security policies

**start>Group Policy Management>domains>*domain name>* settings tab> right click> edit**

Disable IPv6

**ncpa.cpl>uncheck IPv6**

Access Services

**services.msc**

* **Remote Access Connection Manager, Remote Desktop Configuration, Remote Desktop Services, Telnet, IP Telephony, Telnet, Print Spooler, Multimedia Class Scheduler**

Bulk Password Control

http://bit.ly/bulkpasswordcontrol

Verify Signatures

**sigverif**

Update OS

**windows update**

Extras:

* Uninstall Programs
* Bring up firewall
* Install MSE (Must add web page to the trust sites settings)
  + http://windows.microsoft.com/en-us/windows/security-essentials-download
* Update Java and Flash
* MSBA (Microsoft Security Baseline Analyzer)
  + http://www.microsoft.com/en-us/download/details.aspx?id=7558
* SysInternals Suite
  + <https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
    - procexp

### Installations

Install Wireshark

<http://www.wireshark.org/>

MalwareBytes Anti-Malware

<http://www.malwarebytes.org>

CCleaner Optimization and Cleaning

<https://www.piriform.com/ccleaner>

Microsoft Baseline Security Analyzer (MBSA)

<http://www.microsoft.com/en-us/download/details.aspx?id=7558>

Secunia Personal Software Inspector (PSI)

<http://secunia.com/vulnerability_scanning/personal/>

### Network

Netstat –anob

### Account + Password Policy

**Minimum Password Length (15 Characters**)

Start> secpol.msc > Account Policies > Password Policies > Minimum Password Length

**Maximum Password Age (30 days)**

Start> secpol.msc > Account Policies > Password Policies > Maximum Password Age

**Minimum Password Age (5 days)**

Start > secpol.msc > Account Policies > Password Policies > Minimum Password Age

**Enforce Password History (5 passwords remembered)**

Start > secpol.msc > Account Policies > Password Policies > Enforce password history

**Password Complexity**

Start > secpol.msc > Account Policies > Password Policies > Password must meet complexity requirements

**Account Lockout Threshold**

Start > secpol.msc > Account Policies > Account Lockout Policy > Account lockout threshold

### Local Policies

**Audit Policy**

Start > secpol.msc > Local Policies > Audit Policy

**Security Options**

Start > secpol.msc > Local Policies > Security Options

### Remote Access

**Deny remote desktop**

Start > right click Computer > Properties > Remote Settings > Don’t allow remote connections to this computer

**Deny remote assistance**

Start > right click Computer > Properties > Remote Settings > Uncheck Allow Remote Assistance connections to this computer

**Disable remote services**

Start > services.msc

Disable: Remote Access Connection Manager, Remote Desktop Configuration, Remote Desktop Services, Remote Registry

## Windows 8

## Windows 7

### Update

**Download/Install Service Pack 1**

http://www.microsoft.com/en-us/download/details.aspx?id=5842

## Windows XP

### Update

**Download/Install Service Pack 2**

<http://www.microsoft.com/en-us/download/details.aspx?id=28>

**Download/Install Service Pack 1**

http://www.microsoft.com/en-us/download/details.aspx?id=24

## Windows Server 2012

## Windows Server 2008

### Update

**Download/Install Service Pack 1**

http://www.microsoft.com/en-us/download/details.aspx?id=5842

## Windows Server 2003

### Update

**Download/Install Service Pack 1**

<http://www.microsoft.com/en-us/download/details.aspx?id=11435>

**Download/Install Service Pack 2**

http://technet.microsoft.com/en-us/windowsserver/bb229701

Added

Windows Security  
So to Windows, Meterpreter is your biggest threat. If they get ANY access to a Windows system, then you can guarantee they will MIMICATZ it. This means that they will INSTANTLY gain access to every password hash for currently logged in users. If you are accessing Windows boxes with an administrative user, you just got your face pwned – AND they will golden ticket your entire domain – aka, you just lost and have a LOT of repairs to do. To AVOID this, use NON ADMINISTRATIVE accounts for ALL Windows Systems. Then use ‘right click, run as administrator’ to run individual apps with elevated privileges as necessary. This GREATLY reduces your attack surface to this type of attack.  
Also, create an Administrative account (domain and local). Check it works. Then rename and disable the default Administrator (local and domain). Once disabled, create a NEW unprivileged user called ‘Administrator’ with a STRONG password. Turn audit login events on, and start watching your logs for attempts to access the Administrator account. Report this to the black team and score points!

List all sessions connected to this machine  
NET SESSION  
List sessions from a given machine  
NET SESSION \\ComputerName  
Disconnect all sessions connected to this machine  
NET SESSION /DELETE  
Disconnect all sessions connected to this machine (without any prompts)  
NET SESSION /DELETE /y  
Disconnect sessions from a given machine  
NET SESSION \\ComputerName /DELETE

Checking Host : OSSEC is an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.  
PeerBlock- software package that does IP blocking for windows and supports LARGE IP lists (like every IP but my subnet) and supports egress  
Some specific Windows Group Policy to set  
Security Options  
Network security: LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM  
Network security: Do not store LAN Manager hash value on next password change - Enabled  
Network access: Do not allow anonymous enumeration of SAM accounts and shares - Enabled  
Network access: Do not allow anonymous enumeration of SAM accounts - Enabled  
Network access: Allow anonymous SID/name translation - Disabled  
Accounts: Rename administrator account - Rename to something unique (but remember it)  
Interactive logon: Message text for users attempting to log on - sometimes an inject

GENERAL THINGS TO THINK ABOUT

Default passwords (not just on OS, but also webapps, devices such as [power strips](http://ctf.forgottensec.com/wiki/index.php?title=Power_strips&action=edit&redlink=1), [databases](http://ctf.forgottensec.com/wiki/index.php?title=Databases))

Pwnie Express

ASA - Setup and recovery

Backups - Hidden, and hashed to check for changes, DB dump

[Sticky Bits and Immutable Flags](http://ctf.forgottensec.com/wiki/index.php?title=Sticky_Bits_and_Immutable_Flags&action=edit&redlink=1)

Use Nagios as a Pivot Point

|  |
| --- |
|  |