# Quick Start

This is the 80/20 rule in action. This one page of work will keep out the majority of attacks.

Finish this Quick Start list first, then work through the complete list. Time is of the essence. Red Team is already on the prowl.

Some of these steps will take the computer a while to do. I’ve organized them in a way so you can start one and move onto another while the computer downloads/installs things.

## Security

### Accounts

Ctrl+Alt+Del Change a password…

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Security Options

Accounts: Rename administrator account = pick something unique

Accounts: Guest account status - Disabled

### Updates

MS03-026, MS08-067, MS08-069, MS09-050, & MS10-025

CMD: wusa [location of .msu] /quiet /warnrestart

### Use Security Configuration Wizard

Start>Administrative Tools>Security Configuration Wizard

### Network security

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Security Options

Network security: Do not store LAN Manager hash value on next password change = Enabled

Network security: LAN Manager authentication level = Send NTLMv2 response only. refuse NTLM & LM

### Network access

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Security Options

Network access: Allow anonymous SID/name translation = Disabled

Network access: Do not allow anonymous enumeration of SAM accounts = Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares = Enabled

## Audit Policy

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings> Local Policies>Audit Policy

Audit process tracking = Success

Audit account management = Success, Failure

Audit logon events = Success, Failure

Audit account logon events = Success, Failure

### User Rights Assignment

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>User Rights Assignment

Debug programs = Remove all groups/users

Allow log on through Terminal/Remote Desktop Services = Leave blank to disallow login via TS even if it has been started.

### Local GOPs

Export a config from a VM or other default install for reference:

CMD: secedit /export /cfg checkme.inf

Edit to to have more secure settings then import onto your target system:

CMD: secedit /configure /db secedit.sdb /cfg securecheckme.inf