Config for malware lab

Config for Malware Lab:

• Config internal or host only networking
• Configure static IP addresses (if you want 2 different VMs to be able to communicate w/each other, set them both up on the same IP address range)
    ■ The gateway & DNS server should both be the same IP address.
    ■ Both machines should share the same gateway & DNS server IP address
• Guest additions - Might not want to install as some malware checks for this to ensure it's not being ran in analysis environment.
• Setting up Shared Drives
    ■ Safer option is to install CURL & python. Use SimpleHTTPServer
• Disabling password (in VM)
• Disabling firewall (in VM)
• Disabling microsoft defender (in VM)
• Disabling microsoft update (in VM)
• Install monitoring software for malware analysis

Disabling Password:

• open netplwiz
• uncheck “users must enter username & password to use this computer"
• Apply - Reboot to confirm

Disable Firewall:

• Open control panel
• System & security
• Windows Defender Firewall
• Turn Windows Defender Firewall on or off
• Check “Turn off Windows Defender”
• cmd - `netsh advfirewall set allprofiles state off`
• powershell - `Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False`

Disable Defender:

• gpedit.msc
• Computer config > Admin Templates > Windows Components > Windows Defender Antivirus
    ■ Turn off Windows Defender AV
    ■ Select the ENABLED to disable windows defender
    ■ Verify Anti Malware service is disabled too
• Powershell - Set-MpPreference -DisableRealtimeMontioring $true (temporarily disables defender)

Disable Update:

• Control panel
• Admin tools
• services > scroll to “Windows Update” & turn off
• right click & select disable