




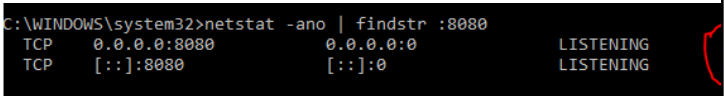
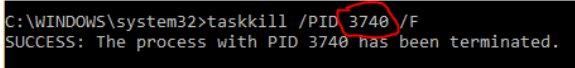
<https://www.youtube.com/watch?v=tfxlgHX9fe8>

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
Telnet client	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
Disable	

Default guest	Disable Rename Password expires User cannot change password
Default Administrator	Disable Rename 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 -
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
Local Security Policy	secpol.msc
Password Policies	Enforce password history: 10 Maximum password age: 90 Minimum password age: 30 Minimum password length: 14 Password must meet complexity requirements: Enabled Store with reversible encryption: Disabled
Account Lockout Policy	Account lockout duration: 30 minutes Account lockout threshold: 10 attempts Reset account lockout counter after: 30 minutes
Local Policy	Audit: Everything Success, Failure
User rights assignment	 user rights assignment
Security Options	Security Options: Do not require CTRL+ALT+DEL [disabled] Security Options: Clear virtual memory page file [enabled] CD-ROM access restricted to locally logged-on users  Security Options (not done but like uh I did the important ones other then network sec, use windows site for more information if necessary)

Services	Turn Off
SNMP Trap	
MOST remote services RPC is necessary	
Server (if not needed)* Scorpio requires the Server service	
IP Helper internet Explorer is uninstalled (feature uninstallation)	
More !!	 Services
Services	Turn On
Windows Firewall Windows Update Windows Defender Windows Event Log	
Shares	fsmgmt.msc
Default shares	ADMIN\$ C\$ IPC\$
Internet Explorer	Click on Gear icon
Security tab	Set all the highest except for trusted site which can be medium
Privacy tab	Cookies set to second highest, or to accept first-party and block third-party Pop-up blocker

Persistence	
Download Malwarebytes	
Task Scheduler	<ul style="list-style-type: none"> - If anything is being repeated check task scheduler - Restart system after turning off

	<ul style="list-style-type: none"> - Make sure to show hidden tasks - Look at the name, the trigger, and the action upon trigger of each active task
GPEDIT	Gpedit.msc
Make	
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
To kill a connection	<p>1) netstat -ano findstr :<PORT> 2) taskkill /PID <PID> /F</p>  <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> <pre>taskkill /PID <PID> /F</pre> <p>(No colon this time)</p>  <p>3)</p>
Server	Will do... but like not much special here
Advanced security	
System	Run > control system >system properties
Computer name	Change description Change network ID <ul style="list-style-type: none"> - Joining workgroup/domain Change computer name/domain
Hardware	Ignore
Advanced	<ul style="list-style-type: none"> - Can change performance - In advanced > advanced <ul style="list-style-type: none"> - Clear virtual memory is here - DEP <ul style="list-style-type: none"> - Turn on for all

System Protection	Set up restore point in case of failure
Remote	No remote assistance Remote Desktop disabled
System config	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	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	Not much here
Monitoring tools	
Performance monitor	Counter - specific measurement for objects Counters exist for cache, memory, paging file, disk, etc.
Windows Registry	Hardest and most obscure
Advanced sharing settings	<ul style="list-style-type: none"> - Turn on file printer sharing - Turn on password
VMware networking	<p>NAT</p> <ul style="list-style-type: none"> • share IP with host • has internet • best option for general use <p>Host-only</p> <ul style="list-style-type: none"> • VM gets own private address • cannot talk to host • no internet unless specific settings are defined • 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
Windows registry	<p>There is a lot on here :</p> <p>https://docs.google.com/presentation/d/1dWLiXJsciiEQMay244QRgdC9K0phM0piqyPoew7PB9s/edit?usp=sharing</p>