

Starting Up

1. If you have not already done it, make a backup copy of Server-1
2. Start Server-1 with VMWare Player
3. Open command tool, run ipconfig to find IP address. IP Address _____
4. On Host, run WinStrobe against your server - What services are running?
5. Copy the fport.exe file to the shared directory on the virtual machine.
6. On Host, start IE, go to http://server_ip_address - Is there a web page running?
7. Start / Settings / Network and Dial Up Connections / Local Area Connection / Properties
8. Select TCP/IP properties, select "use the following IP address"
9. Set IP address to current address, subnet to 255.255.255.0
10. Select Advanced / WINS, Disable NetBIOS over TCP/IP

Disabling Services

11. On Host, run WinStrobe against your server - What services are running? Is there a difference?
12. Start / Settings / Control Panel / Add/Remove Programs / Add/Remove Windows Components
13. Uncheck EVERYTHING, select Next. Wait until finished
14. On Host, start IE, go to http://server_ip_address - did you get an error?
15. On Host, run WinStrobe against your server - What services are running? Is there a difference?
16. Start / Setting / Control Panel / Administrative Tools / Services
17. Disable and Stop all services except

1	DNS Client*
2	EventLog*
3	IPSec Policy Agent
4	Logical Disk Manager*
5	Network Connections
6	Plug & Play*
7	Protected Storage*
8	Remote Procedure Call
9	Remote Registry Service
10	RunAs Service
11	Security Accounts Manager*
12	VMware Tools Service ???

(*) indicates minimal services required to operate

Double click each service NOT listed above, set Startup Type to Disabled, and STOP service if running

18. Reboot the virtual machine
19. On Host, run WinStrobe against your server - What services are running? Is there a difference?
20. On the Server open a command tool. Enter the command> d :
21. Enter the command> cd shared
22. Enter the command> fport
23. What services are running? How does it compare to WinStrobe?

Tightening the System

24. Start / Programs / Administrative Tools / Local Security Policy
25. Expand Account Policies
26. Select Password Policy
27. Set the following values

Enforce Password History	Enabled (value is 24)
Maximum Password Age	Enabled (value is 90)
Minimum Password Age	Enabled (value is 1)
Minimum Password Length	Enabled (value is 8)
Password Must Meet Complexity Requirements	Enabled
Store Passwords Using Reversible Encryption	Disabled

28. Select Account Lockout Policy
29. Set the following values

Account Lockout Duration	Enabled (value is 15)
Account Lockout Threshold	Enabled (value is 3)
Reset Account Lockout counter	Enabled (value is 15)

30. Expand Local Policies
31. Select Audit Policy
32. Set the following values

Audit Account Login Events	Success, Failure
Audit Account Management	Success, Failure
Audit Directory Service Access	Failure
Audit Logon Events	Success, Failure
Audit Object Access	Failure
Audit Policy Change	Success, Failure
Audit Privilege Use	Failure
Audit Process Tracking	No Auditing
Audit System Events	Success, Failure

33. Select Security Options
34. Set the following values

Additional Restrictions for Anonymous Connections	No Access without explicit anonymous permissions
Allow system to be shut down without having to log in	Disabled
Audit use of backup and restore privilege	Enabled

Clear virtual memory pagefile when system shuts down	Enabled
Digitally Sign Client Communications (Always)	Enabled (for high security)
Digitally Sign Client Communications (When Possible)	Enabled (for medium security)
Digitally Sign Server Communications (Always)	Enabled (for high security)
Digitally Sign Server Communications (When Possible)	Enabled (for medium security)
Disable CTRL-ALT-DEL requirement for logon	Disabled
Do Not display last user name in logon screen	Enabled (for multi-user system)
LAN Manager Authentication Level	Send NTLMv2 responses only/refuse LM & NTLM
Message text for user attempting to log on	Authorized Users Only
Message title for user attempting to log on	Company Warning Statement
Number of previous logons to cache (in case domain controller is not available)	0
Prevent user from installing printer drivers	Enabled
Recovery console: allow automatic administrative logon	Disabled
Rename Administrator account	admin1
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict Floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (Always)	Enabled (for high security)
Secure channel: Digitally encrypt secure secure channel data (When possible)	Enabled (for medium-high security)
Secure channel: Digitally sign secure channel data (When possible)	Enabled (for medium security)
Secure channel: require strong (Windows 2000 or later) Session key	Enabled (for ultra-high security)
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut Down System Immediately if unable to log security audits	Enabled
Strength default permissions of Global System Objects (e.g. Symbolic links)	Enabled
Unsigned Driver Installation Behavior	Do not allow installation
Unsigned Non-Driver Installation Behavior	Do not allow installation

35. Close Local Security Settings
36. Shutdown and Restart

Install IIS and FTP

37. Start / Settings / Control Pane / Add/Remove Programs / Add/Remove Windows Components
38. Highlight (do not select) Internet Information Services and click Details
39. Select the following
 - a. Common Files
 - b. Documentation
 - c. File Transfer Protocol
 - d. IIS Snap-In
 - e. WWW Server
40. Click OK and Next
41. On Host, run WinStrobe against your server - What services are running? Is there a difference?
42. On Host, start IE, go to http://server_ip_address - Is there a web page running?
43. Go to folder c:\inetpub\wwwroot
44. Right click, New, text document, Enter some text, save it as default.htm
45. On Host, in IE, reload the page - Is there a web page running?
46. If there are other ports responding, test them with telnet - can you establish a connection?
47. Run Retina against the server. What results do you get?