

DOWNLOAD THIS FILE AND PUT IT IN C:\ BEFORE RUNNING SCRIPT

MAKE SURE TO REMOVE THE .TXT AT THE END

<https://www.mediafire.com/file/f46g301n1tj3w0d/policies.inf/file>

To get SHA 256 or other hashes

- Shift + right click in files folder then open with powershell
Get-FileHash -Algorithm SHA256 .filename.extension

Local group policy editor

Security settings

Local policy

Change audit policies

- Enforce password history 3-5
- Max password age 90 days
- Minimum password age 30 days
- Minimum password length 10
- Password meet complexity enabled
- Store passwords disabled.

Change security options

- Disable admin account status and guest
- Enable limit local account use
- Disable Restrict Cd-Rom access to locally logged on users
- Enable restrict floppy access
- Enable LDAP server signing
- Enable Don't display sign in
- Disable not require ctrl alt del
- Enable digitally sign communications
- Disable send an unencrypted password
- Enable digitally sign communications
- Disable allow anonymous SID

Account lockout policy

- Account lockout threshold 5 attempts
- other 2 things 30mins

Attach Detection

- Task Scheduler & Task Manager
- Monitor Performance and Resource Usage
- Port Checks
- Event Viewer

Delete Suspicious Files

Look in C:\Windows\System & C:\Windows\System32 for programs with recent timestamps

Disable Simple TCP/IP servicesIn the Search box

type gpedit.msc. Expand Computer Configuration → expand Administrative

Templates → expand Windows Components → expand Remote Desktop

Services → expand Remote Desktop Session Host → double-click on

Connections → double-click on Allow Users to connect remotely by using Remote

Desktop Services → select Disabled → select Apply → select OK

Go to **fsmgmt.msc** and find SUS! Shares

Lusrmgr.msc for groups

Command	Opens the command prompt .
Compmgmt.msc	Opens the computer management console.
Devmgmt.msc	Opens the device manager.
Diskmgmt.msc	Opens the disk management tool.
Eventvwr.msc	Opens the event viewer.
Fsmgmt.msc	Opens shared folders.
Gpedit.msc	Opens the group policy editor.
Lusrmgr.msc	Opens the local users and groups.
Mailto:	Opens the default email client.
Msconfig	Opens the system configuration utility.

Msinfo32	Opens the system information utility.
Perfmon.msc	Opens the performance monitor.
Regedit	Opens the registry editor.
Rsof.msc	Opens resultant set of policy.
Secpol.msc	Opens local security settings.
Services.msc	Opens services utility.
System.ini	Windows loading information.
Win.ini	Windows loading information.
Winver	Shows current version of Windows.

Forensics Question 1 correct - 8 pts
 Forensics Question 2 correct - 8 pts
 Removed unauthorized user tamatoa - 4 pts
 Removed unauthorized user kakamora - 4 pts
 User heihei is not an administrator - 4 pts
 User minimaui is not an administrator - 4 pts
 Changed insecure password for maui - 4 pts
 Updated users in voyagers group - 5 pts
 A secure minimum password length is required - 4 pts
 Passwords are not stored using reversible encryption - 4 pts
 Do not require CTRL+ALT+DEL [disabled] - 4 pts
 Firewall protection has been enabled - 5 pts
 Remote Registry service has been stopped and disabled - 5 pts
 The majority of Windows updates are installed - 5 pts
 Firefox has been updated - 5 pts
 Prohibited MP3 files are removed - 5 pts
 Removed TV 3L PC - 4 pts

Removed Wireshark - 4 pts
Removed Hash Suite - 5 pts
Firefox pop-up blocker enabled - 5 pts

Remote assistance

S3@shell

Forensics Question 1 correct - 7 pts
Forensics Question 2 correct - 7 pts
Guest account is not enabled - 3 pts
Removed unauthorized user hjannerone - 3 pts
Removed unauthorized user ncardigan - 3 pts
User shudson is not an administrator - 3 pts
User mpalmer has a password - 2 pts

Passwords expire lusrmgr.msc

A secure lockout threshold exists - 3 pts
A secure account lockout duration exists - 3 pts
Limit local use of blank passwords to console only [enabled] - 2 pt
Recovery console: Allow automatic administrative logon [disabled] - 3 pts
Audit Logon [Success] - 3 pts
Audit User Account Management [Success] - 3 pts
Remote Desktop sharing is disabled - 4 pts
The majority of Windows updates are installed - 3 pts

Update GnuCash

Removed prohibited MP3s - 3 pts
Removed Torrent Video Player - 3 pts
Removed OpenRA games - 3 pts
Removed Cabos P2P application - 3 pts
Removed narc backdoor - 4 pts
Windows SmartScreen configured to warn or block - 3 pts
Firefox blocks dangerous downloads - 3 pts

Windows state

Forensics Question 1 correct - 7 pts
Forensics Question 2 correct - 7 pts
Forensics Question 3 correct - 7 pts
Removed unauthorized user poi - 2 pts
Removed unauthorized user te'ka - 2 pts
User ocean has administrator privileges restored - 3 pts
Remote Desktop Users group includes all authorized users - 3 pts
User lua has a password - 2 pts
A secure lockout threshold exists - 3 pts
A sufficient password history is being kept - 2 pts
Audit Audit Policy Change [Success] - 3 pts
Behavior of the elevation prompt for administrators in Admin Approval Mode configured to prompt - 3 pts
Firewall protection has been enabled - 3 pts
Windows Event Log service is running - 4 pts
Simple TCP/IP Services have been stopped and disabled - 3 pts
The majority of Windows updates are installed - 3 pts
OpenCPN has been updated - 3 pts
Removed mimikatz archive - 4 pts
Removed Steam - 2 pts
Removed Runescape - 2 pts
Removed Actual Keylogger - 4 pts
Removed WindowsRAT - 4 pts
Google Chrome safe browsing enabled - 3 pts
Google Chrome HTTPS-Only mode enabled - 2 pts

SERVER:











Forensics Question 1 correct - 7 pts
Forensics Question 2 correct - 7 pts
Forensics Question 3 correct - 7 pts
Removed unauthorized user dcordray - 3 pts
Removed unauthorized user hunter - 3 pts
User dschrute is not an administrator - 4 pts












User kmalone has a password - 3 pts
 Changed insecure password for lozenge - 4 pts
 A sufficient password history is being kept - 3 pts
 Passwords must meet complexity requirements - 3 pts
 Audit Computer Account Management [Success] - 4 pts
 Firewall protection has been enabled - 3 pts
 The majority of Windows updates are installed - 3 pts
 7-Zip has been updated - 4 pts
 Removed Printer Exploitation Toolkit (PRET) archive - 4 pts
 Removed Print Spooler research and exploit archive - 5 pts
 Removed plain text file with passwords in it - 4 pts
 Removed Geneforge - 4 pts
 Removed LizardSystems Wi-Fi Scanner - 4 pts
 Firefox warns when sites try to install add-ons - 5 pts

Set audit policies to success and failure

Lusrmgr.msc - edit local user group policies

CertUtil -hashfile yourFileName MD5

	Simple TCPIP services (i.e. echo, daytime etc)	
	Audit account logon events	Success, Failure
	Audit account management	Success, Failure
	Audit directory service access	Success, Failure
	Audit logon events	Success, Failure
	Audit object access	Success, Failure
	Audit policy change	Success, Failure
	Audit privilege use	Success, Failure
	Audit process tracking	Success, Failure
	Audit system events	Success, Failure

 Enforce password history	5 passwords remembered
 Maximum password age	90 days
 Minimum password age	30 days
 Minimum password length	10 characters
 Minimum password length audit	Not Defined
 Password must meet complexity requirements	Enabled
 Relax minimum password length limits	Not Defined
 Store passwords using reversible encryption	Disabled
 Account lockout duration	30 minutes
 Account lockout threshold	5 invalid logon attempts
 Reset account lockout counter after	30 minutes

```
@echo off
Title Main Run
Color 0A
echo Admin Check?!?!?!!!!
net sessions
if %errorlevel%==0 (
echo Admin Access Granted
echo PRESS ENTER
) else (
echo Use admin dummy
pause
exit
)
:MENU
cls
echo Choose An option:
echo 1. A bunch of auto stuff that does thing automatically
echo 2. REMOTE DESKTOP
echo 3. Download updated versions for Malwarebytes and Firefox
echo 4. AUDIT
echo 5. Guest and admin bye bye
echo 6. Check the file system
echo 7. Find the forbidden media (Do after forensic questions if they require files)
echo 8. Clear host file
echo 9. NEW USERS SCRIPT TESTING

CHOICE /C 123456789 /M "Enter your choice:"
if ERRORLEVEL A goto
if ERRORLEVEL 9 goto Nine
if ERRORLEVEL 8 goto Eight
if ERRORLEVEL 7 goto Seven
if ERRORLEVEL 6 goto Six
if ERRORLEVEL 5 goto Five
if ERRORLEVEL 4 goto Four
if ERRORLEVEL 3 goto Three
if ERRORLEVEL 2 goto Two
if ERRORLEVEL 1 goto One

:One
echo Showing hidden files
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Hidden /t REG_DWORD /d 1 /f
echo showing super hidden files
```



```

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowSuperHidden /t REG_DWORD /d 1 /f
echo showing file extensions
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v HideFileExt /t REG_DWORD /d 0 /f
echo showing file check boxes
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /V AutoCheckSelect /T
REG_DWORD /D 1 /F
echo RESTARTING FILE EXPLORER
powershell -c gps 'explorer' ^| stop-process
echo Enabling firewall
netsh advfirewall set allprofiles state on
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t
REG_DWORD /d 3 /f
echo Turning on UAC
reg ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 1 /f
echo Flushing DNS
ipconfig /flushdns
echo Services time
net start
dism /online /disable-feature /featurename:IIS-WebServerRole
dism /online /disable-feature /featurename:IIS-WebServer
dism /online /disable-feature /featurename:IIS-CommonHttpFeatures
dism /online /disable-feature /featurename:IIS-HttpErrors
dism /online /disable-feature /featurename:IIS-HttpRedirect
dism /online /disable-feature /featurename:IIS-ApplicationDevelopment
dism /online /disable-feature /featurename:IIS-NetFxExtensibility
dism /online /disable-feature /featurename:IIS-NetFxExtensibility45
dism /online /disable-feature /featurename:IIS-HealthAndDiagnostics
dism /online /disable-feature /featurename:IIS-HttpLogging
dism /online /disable-feature /featurename:IIS-LoggingLibraries
dism /online /disable-feature /featurename:IIS-RequestMonitor
dism /online /disable-feature /featurename:IIS-HttpTracing
dism /online /disable-feature /featurename:IIS-Security
dism /online /disable-feature /featurename:IIS-URLAuthorization
dism /online /disable-feature /featurename:IIS-RequestFiltering
dism /online /disable-feature /featurename:IIS-IPSecurity
dism /online /disable-feature /featurename:IIS-Performance
dism /online /disable-feature /featurename:IIS-HttpCompressionDynamic
dism /online /disable-feature /featurename:IIS-WebServerManagementTools
dism /online /disable-feature /featurename:IIS-ManagementScriptingTools
dism /online /disable-feature /featurename:IIS-IIS6ManagementCompatibility
dism /online /disable-feature /featurename:IIS-Metabase
dism /online /disable-feature /featurename:IIS-HostableWebCore
dism /online /disable-feature /featurename:IIS-StaticContent
dism /online /disable-feature /featurename:IIS-DefaultDocument
dism /online /disable-feature /featurename:IIS-DirectoryBrowsing
dism /online /disable-feature /featurename:IIS-WebDAV
dism /online /disable-feature /featurename:IIS-WebSockets
dism /online /disable-feature /featurename:IIS-ApplicationInit
dism /online /disable-feature /featurename:IIS-ASPNET
dism /online /disable-feature /featurename:IIS-ASPNET45
dism /online /disable-feature /featurename:IIS-ASP
dism /online /disable-feature /featurename:IIS-CGI
dism /online /disable-feature /featurename:IIS-ISAPIExtensions
dism /online /disable-feature /featurename:IIS-ISAPIFilter
dism /online /disable-feature /featurename:IIS-ServerSideIncludes
dism /online /disable-feature /featurename:IIS-CustomLogging
dism /online /disable-feature /featurename:IIS-BasicAuthentication
dism /online /disable-feature /featurename:IIS-HttpCompressionStatic
dism /online /disable-feature /featurename:IIS-ManagementConsole
dism /online /disable-feature /featurename:IIS-ManagementService
dism /online /disable-feature /featurename:IIS-WMICompatibility

```

```
dism /online /disable-feature /featurename:IIS-LegacyScripts
dism /online /disable-feature /featurename:IIS-LegacySnapIn
dism /online /disable-feature /featurename:IIS-FTPService
dism /online /disable-feature /featurename:IIS-FTPSvc
dism /online /disable-feature /featurename:IIS-FTPExtensibility
dism /online /disable-feature /featurename:TFTP
DISM /online /disable-feature /featurename:TelnetClient
DISM /online /disable-feature /featurename:TelnetServer
sc stop "TintSvr"
sc config "TintSvr" start= disabled
```

```
echo PRESS ENTER TO GO TO MENU
goto MENU
```

:Two

```
echo Disabling remote desktop...
sc stop "TermService"
sc config "TermService" start= disabled
sc stop "SessionEnv"
sc config "SessionEnv" start= disabled
sc stop "UmRdpService"
sc config "UmRdpService" start= disabled
sc stop "RemoteRegistry"
sc config "RemoteRegistry" start= disabled
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v AllowTSConnections /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowToGetHelp /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t
REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="remote desktop" new enable=no
```

```
echo PRESS ENTER TO GO TO MENU
goto MENU
```

:THREE

```
set CCD=%CD%
cd "C:\Users\%username%\Downloads"
powershell -Command "Invoke-WebRequest 'https://download.mozilla.org/?product=firefox-latest&os=win64&lang=en-US'
-OutFile firefox-lat.exe"
powershell -Command "Invoke-WebRequest
'https://data-cdn.mbamupdates.com/web/affiliate_builds/win_temp/MBSetup-119967.119967-consumer.exe' -OutFile
malwarebytes-lat.exe"
start "" firefox-lat.exe
start "" malwarebytes-lat.exe
cd %CCD%
```

```
echo PRESS ENTER TO GO TO MENU
goto MENU
```

:Four

```
secedit.exe /configure /db %windir%\security\local.sdb /cfg E:\policies.inf
```

```
echo Current:
```

```
net accounts
```

```
echo PRESS ENTER TO GO TO MENU
goto MENU
```

```
:Five
```

```
net user guest /active:no
net user admin /active:no
```

```
echo PRESS ENTER TO GO TO MENU
goto MENU
```

```
:Six
echo Scanning now.....
Sfc.exe /scannow
```

```
echo PRESS ENTER TO GO TO MENU
goto MENU
```

```
:Seven
@echo off
cls
echo Flashing disk
dir /b /s "C:\Program Files\" > programfiles.flashed
dir /b /s "C:\Program Files (x86)\\" >> programfiles.flashed
dir /b /s "C:\Users\" > users.flashed
dir /b /s "C:\Documents and Settings\" >> users.flashed
echo User profiles flashed
dir /b /s "C:\\" > c.flashed
echo Done flashing
echo Finding media files in C:\Users and/or C:\Documents and Settings...
findstr .mp3 users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.mp3 > media_audio
findstr .ac3 users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.ac3 >> media_audio
findstr .aac users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.aac >> media_audio
findstr .aiff users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.aiff >> media_audio
findstr .flac users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.flac >> media_audio
findstr .m4a users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.m4a >> media_audio
findstr .m4p users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.m4p >> media_audio
findstr .midi users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.midi >> media_audio
findstr .mp2 users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.mp2 >> media_audio
findstr .m3u users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.m3u >> media_audio
findstr .ogg users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.ogg >> media_audio
findstr .vqf users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.vqf >> media_audio
findstr .wav users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.wav >> media_audio
findstr .wma users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.wma >> media_video
findstr .mp4 users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.mp4 >> media_video
findstr .avi users.flashed >NUL
```

```

if %errorlevel%==0 where /r c:\Users\ *.avi >> media_video
findstr .mpeg4 users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ .mpeg4 >> media_video
findstr .gif users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.gif >> media_pics
findstr .png users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.png >> media_pics
findstr .bmp users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ *.bmp >> media_pics
findstr .jpg users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ .jpg >> media_pics
findstr .jpeg users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ .jpeg >> media_pics
findstr .txt users.flashed >NUL
if %errorlevel%==0 where /r c:\Users\ .txt >> txt
C:\WINDOWS\system32\notepad.exe media_video
C:\WINDOWS\system32\notepad.exe media_audio
C:\WINDOWS\system32\notepad.exe media_pics
C:\WINDOWS\system32\notepad.exe txt_files
echo Searching for hacking tools (Will not auto delete do that yourself)
findstr "Cain" programfiles.flashed
if %errorlevel%==0 (
echo Cain detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "nmap" programfiles.flashed
if %errorlevel%==0 (
echo Nmap detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "keylogger" programfiles.flashed
if %errorlevel%==0 (
echo Potential keylogger detected. Please take note, then press any key.
pause >NUL
)
findstr "CCleaner" programfiles.flashed
if %errorlevel%==0 (
echo CCleaner detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "Armitage" programfiles.flashed
if %errorlevel%==0 (
echo Potential Armitage detected. Please take note, then press any key.
pause >NUL
)
findstr "Wireshark" programfiles.flashed
if %errorlevel%==0 (
echo Wireshark detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "npcap" programfiles.flashed
if %errorlevel%==0 (
echo npcap detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "Metasploit" programfiles.flashed

```

```
if %errorlevel%==0 (
echo Potential Metasploit framework detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "BitTorrent" programfiles.flashed
if %errorlevel%==0 (
echo BitTorrent detected. Please take note, then press any key.
pause >NUL
)
cls
findstr "Shellter" programfiles.flashed
if %errorlevel%==0 (
echo Potential Shellter detected. Please take note, then press any key.
pause >NUL
)
cls
goto MENU
```

:Eight

```
echo Clearing Host file
attrib -r -s C:\WINDOWS\system32\drivers\etc\hosts
echo > C:\Windows\System32\drivers\etc\hosts
if %errorlevel%==0 echo Host file sucessfully cleared
if %errorlevel%==1 echo ERROR
pause
```

goto MENU

:Nine

```
wmic /output:C:\Username.txt useraccount get name
wmic /output:C:\Userdetails.txt useraccount list full
C:\Username.txt
pause
```

gotoMENU

```
net accounts /minpwlen:10
net accounts /maxpwage:90
net accounts /minpwage:30
net accounts /lockoutthreshold:5
```

```
net user username /delete
net user
Net Localgroup Administrators NAME /add
```

Net Localgroup Administrators NAME /Delete

```
@echo off
Title Fortnite
Color 0A
echo Admin Check?!?!?!!!!
net sessions
if %errorlevel%==0 (
echo Admin Access Granted
echo PRESS ENTER
) else (
echo Use admin dummy
pause
exit
)
:MENU
pause
cls
echo Chose and option
echo 1. Admin
echo 2. Users
echo 3. Delete Accounts

CHOICE /C 123 /M "Enter your choice:"
if ERRORLEVEL 3 goto Three
if ERRORLEVEL 2 goto Two
if ERRORLEVEL 1 goto One

:One
set /p Var="Amount of Admins: "
FOR /L %%G IN (1,1,%Var%) DO goto Admin

goto MENU
```

```

:Admin
set /a "x = 1"
:adminLoop
if %x% leq %Var% (
    set /p Admin="Admin Name: "
    Net Localgroup Administrators %Admin% /add
    set /a "x = x + 1"
    goto :adminLoop
)
goto MENU

```

```

:Two
set /p Var="Amount of Users: "
FOR /L %%G IN (1,1,%Var%) DO goto User

```

```

goto MENU

```

```

:User
set /a "x = 1"
:UserLoop
if %x% leq %Var% (
    set /p User="Enter name to set as user: "
    Net Localgroup Administrators %User% /Delete
    set /a "x = x + 1"
    goto :userLoop
)
goto MENU

```

```

set /p User="Enter name to set as user: "
Net Localgroup Administrators %User% /Delete

```

```

goto MENU

```

```

:Three
set /p Bad="Enter User to Delete: "
net user %Bad% /delete

```

```

goto MENU

```

```

@echo off
color 0B
title USERS
cd C:\
(
    Set /p Line_1=
    Set /p Line_2=
    Set /p Line_3=
    Set /p Line_4=
    Set /p Line_5=
    Set /p Line_6=
    Set /p Line_7=
    Set /p Line_8=
    Set /p Line_9=
    Set /p Line_10=
    Set /p Line_11=

```

```
Set /p Line_12=
Set /p Line_13=
Set /p Line_14=
Set /p Line_15=
Set /p Line_16=
Set /p Line_17=
Set /p Line_18=
Set /p Line_19=
Set /p Line_20=
) <Test.txt
```

```
net user %Line_1% Ba11sInYoJaws#1
net user %Line_2% Ba11sInYoJaws#1
net user %Line_3% Ba11sInYoJaws#1
net user %Line_4% Ba11sInYoJaws#1
net user %Line_5% Ba11sInYoJaws#1
net user %Line_6% Ba11sInYoJaws#1
net user %Line_7% Ba11sInYoJaws#1
net user %Line_8% Ba11sInYoJaws#1
net user %Line_9% Ba11sInYoJaws#1
net user %Line_10% Ba11sInYoJaws#1
net user %Line_11% Ba11sInYoJaws#1
net user %Line_12% Ba11sInYoJaws#1
net user %Line_13% Ba11sInYoJaws#1
net user %Line_14% Ba11sInYoJaws#1
net user %Line_15% Ba11sInYoJaws#1
net user %Line_16% Ba11sInYoJaws#1
net user %Line_17% Ba11sInYoJaws#1
net user %Line_18% Ba11sInYoJaws#1
net user %Line_19% Ba11sInYoJaws#1
net user %Line_20% Ba11sInYoJaws#1
Net Localgroup Administrators %Line_1% /Delete
Net Localgroup Administrators %Line_2% /Delete
Net Localgroup Administrators %Line_3% /Delete
Net Localgroup Administrators %Line_4% /Delete
Net Localgroup Administrators %Line_5% /Delete
Net Localgroup Administrators %Line_6% /Delete
Net Localgroup Administrators %Line_7% /Delete
Net Localgroup Administrators %Line_8% /Delete
Net Localgroup Administrators %Line_9% /Delete
Net Localgroup Administrators %Line_10% /Delete
Net Localgroup Administrators %Line_11% /Delete
Net Localgroup Administrators %Line_12% /Delete
Net Localgroup Administrators %Line_13% /Delete
Net Localgroup Administrators %Line_14% /Delete
Net Localgroup Administrators %Line_15% /Delete
Net Localgroup Administrators %Line_16% /Delete
Net Localgroup Administrators %Line_17% /Delete
Net Localgroup Administrators %Line_18% /Delete
Net Localgroup Administrators %Line_19% /Delete
Net Localgroup Administrators %Line_20% /Delete
```

:MENU

echo Choose An option:

```
echo 1. %Line_1%
echo 2. %Line_2%
echo 3. %Line_3%
echo 4. %Line_4%
echo 5. %Line_5%
echo 6. %Line_6%
echo 7. %Line_7%
```



```
echo 8. %Line_8%
echo 9. %Line_9%
echo 0. %Line_10%
echo A. %Line_11%
echo B. %Line_12%
echo C. %Line_13%
echo D. %Line_14%
echo E. %Line_15%
echo F. %Line_16%
echo G. %Line_17%
echo H. %Line_18%
echo I. %Line_19%
echo J. %Line_20%
```

```
CHOICE /C 1234567890ABCDEFGHIJ /M "Who is an admin:"
```

```
if ERRORLEVEL J goto JJ
if ERRORLEVEL I goto II
if ERRORLEVEL H goto HH
if ERRORLEVEL G goto GG
if ERRORLEVEL F goto FF
if ERRORLEVEL E goto EE
if ERRORLEVEL D goto DD
if ERRORLEVEL C goto CC
if ERRORLEVEL B goto BB
if ERRORLEVEL A goto AA
if ERRORLEVEL 0 goto Zero
if ERRORLEVEL 9 goto Nine
if ERRORLEVEL 8 goto Eight
if ERRORLEVEL 7 goto Seven
if ERRORLEVEL 6 goto Six
if ERRORLEVEL 5 goto Five
if ERRORLEVEL 4 goto Four
if ERRORLEVEL 3 goto Three
if ERRORLEVEL 2 goto Two
if ERRORLEVEL 1 goto One
```

```
:One
echo Are you sure you want %Line_1% to be an admin?
pause
Net Localgroup Administrators %Line_1% /add
goto MENU

:Two
echo Are you sure you want %Line_2% to be an admin?
pause
Net Localgroup Administrators %Line_2% /add
goto MENU

:Three
echo Are you sure you want %Line_3% to be an admin?
pause
Net Localgroup Administrators %Line_3% /add
goto MENU

:Four
echo Are you sure you want %Line_4% to be an admin?
pause
Net Localgroup Administrators %Line_4% /add
goto MENU

:Five
echo Are you sure you want %Line_5% to be an admin?
pause
Net Localgroup Administrators %Line_5% /add
goto MENU
```

```
:Six
echo Are you sure you want %Line_6% to be an admin?
pause
Net Localgroup Administrators %Line_6% /add
goto MENU
:Seven
echo Are you sure you want %Line_7% to be an admin?
pause
Net Localgroup Administrators %Line_7% /add
goto MENU
:Eight
echo Are you sure you want %Line_8% to be an admin?
pause
Net Localgroup Administrators %Line_8% /add
goto MENU
:Nine
echo Are you sure you want %Line_9% to be an admin?
pause
Net Localgroup Administrators %Line_9% /add
goto MENU
:Zero
echo Are you sure you want %Line_10% to be an admin?
pause
Net Localgroup Administrators %Line_10% /add
goto MENU
:AA
echo Are you sure you want %Line_11% to be an admin?
pause
Net Localgroup Administrators %Line_11% /add
goto MENU
:BB
echo Are you sure you want %Line_12% to be an admin?
pause
Net Localgroup Administrators %Line_12% /add
goto MENU
:CC
echo Are you sure you want %Line_13% to be an admin?
pause
Net Localgroup Administrators %Line_13% /add
goto MENU
:DD
echo Are you sure you want %Line_14% to be an admin?
pause
Net Localgroup Administrators %Line_14% /add
goto MENU
:EE
echo Are you sure you want %Line_15% to be an admin?
pause
Net Localgroup Administrators %Line_15% /add
goto MENU
:FF
echo Are you sure you want %Line_16% to be an admin?
pause
Net Localgroup Administrators %Line_16% /add
goto MENU
:GG
echo Are you sure you want %Line_17% to be an admin?
pause
Net Localgroup Administrators %Line_17% /add
goto MENU
:HH
```

```
echo Are you sure you want %Line_18% to be an admin?
pause
Net Localgroup Administrators %Line_18% /add
goto MENU
:II
echo Are you sure you want %Line_19% to be an admin?
pause
Net Localgroup Administrators %Line_19% /add
goto MENU
:JJ
echo Are you sure you want %Line_20% to be an admin?
pause
Net Localgroup Administrators %Line_20% /add
goto MENU
```