LAB MANUAL

COMPUTER DATA SECURITY & PRIVACY

(COMP-324)

Course Coordinator: Dr. Sherif Tawfik Amin

Prepared By: Dr. Shadab Alam

(DRAFT Version)

Department of Computer Science
College of Computer Science & Information Systems, Jazan University, Jazan, KSA

SECTION: A

COMMANDS

(This section has windows based commands used for investigating and configuring the computer network.)

Prepared By: **Dr. Shadab Alam**

Some important commands for Data and Network Security

1. **ipconfig:** Configure IP (Internet Protocol configuration)

It displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays the IP address, subnet mask, and default gateway for all adapters.

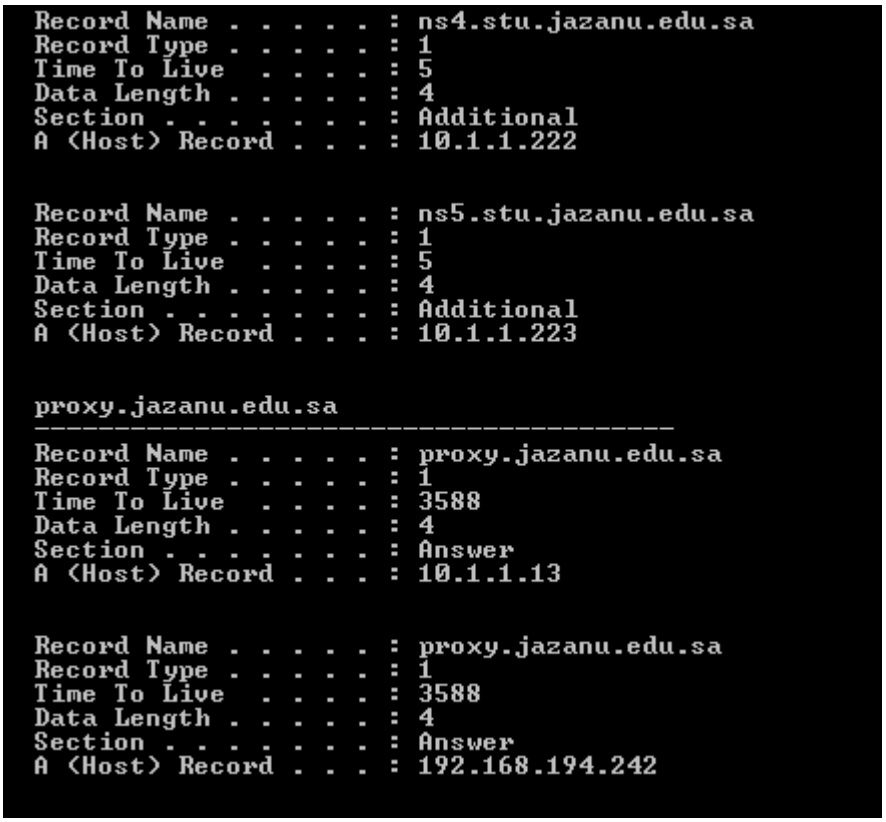
a. **ipconfig:** Display IP configuration.

```
C:\Users\snafis>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2dde:28b9:ce7f:bdb7%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : jazanu.edu.sa
```

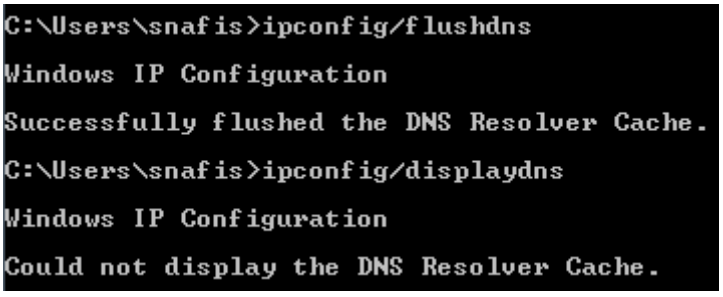
b. **ipconfig /all :** Display full configuration information.

```
C:\Users\snafis>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CCIS-snafis
   Primary Dns Suffix  . . . . . . . : jazanu.edu.sa
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : jazanu.edu.sa

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 2x2 11b/g/n Wireless LAN M.2 Adapter
   Physical Address. . . . . . . . . : 80-56-F2-41-D6-03
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2dde:28b9:ce7f:bdb7%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 16 October 2016 09:15:47
   Lease Expires . . . . . . . . . . : 16 October 2016 11:15:49
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 355738503
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-76-64-FF-28-D2-44-30-FF-7A

   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

c. **ipconfig/displaydns:** That command displays your "local" DNS cache that is stored in Windows, this makes browsing faster because it keeps records for any website you have visited before, on your local hard drive, which means the browser does not have to wait for a DNS server out on the internet to resolve the address and pass that information back to your browser.



d. **ipconfig/flushdns:** Clean the DNS Resolver cache.



2. Ping:

The **ping** command helps to verify IP-level connectivity. When troubleshooting, you can use **ping** to send an ICMP echo request to a target host name or IP address. Use **ping** whenever you need to verify that a host computer can connect to the TCP/IP network and network resources. You can also use **ping** to isolate network hardware problems and incompatible configurations.

Follow this sequence to diagnose network connectivity:

1. Ping the loopback address to verify that TCP/IP is configured correctly on the local computer. **ping 127.0.0.1**
2. Ping the IP address of the local computer to verify that it was added to the network correctly. **ping** *IP_address_of_local_host*
3. Ping the IP address of the default gateway to verify that the default gateway is functioning and that you can communicate with a local host on the local network.

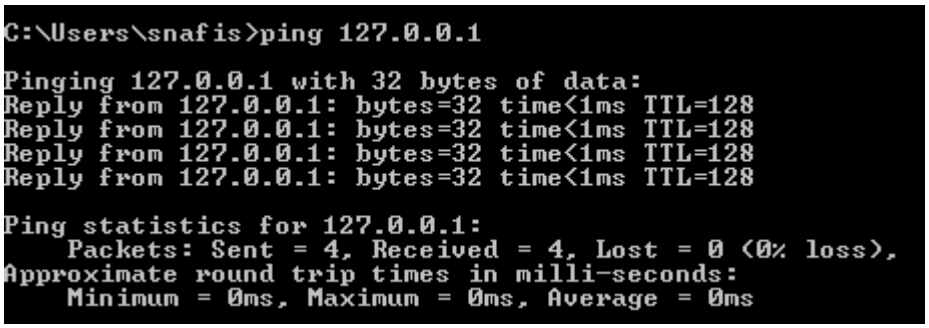
   ping *IP_address_of_default_gateway*
4. Ping the IP address of a remote host to verify that you can communicate through a router.

   ping *IP_address_of_remote_host*

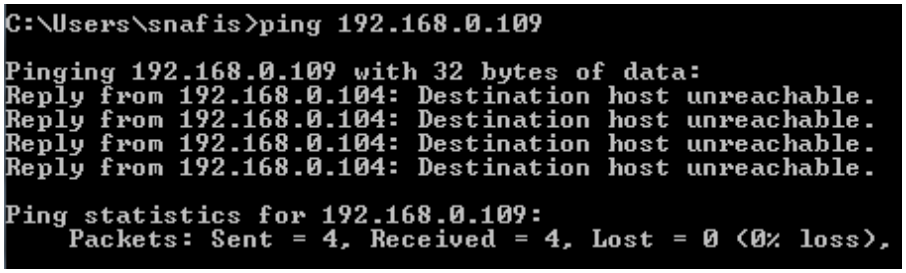
The following table shows some useful **ping** command options.

Option	Use
-n *Count*	Determines the number of echo requests to send. The default is 4 requests.
-w *Timeout*	Enables you to adjust the timeout (in milliseconds). The default is 4,000 (a 4-second timeout).
-l *Size*	Enables you to adjust the size of the ping packet. The default size is 32 bytes.
-f	Sets the Do Not Fragment bit on the ping packet. By default, the ping packet allows fragmentation.
/?	Provides command Help.

If connected or reachable:



If not connected or unreachable:



3. tracert

The tracert command is used to visually see a network packet being sent and received and the amount of hops required for that packet to get to its destination.

Tracert syntax

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:

-d	Do not resolve addresses to hostnames.
-h maximum_hops	Maximum number of hops to search for target. Default is 30 hops.
-j host-list	Loose source route along host-list (IPv4-only).
-w timeout	Wait timeout milliseconds for each reply.
-R	Trace round-trip path (IPv6-only).
-S srcaddr	Source address to use (IPv6-only).
-4	Force using IPv4.
-6	Force using IPv6.

If not connected or unreachable:

```
C:\Users\snafis>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  192.168.0.1
  2  192.168.57.1  reports: Destination net unreachable.

Trace complete.
```

If connected or reachable:

```
C:\Users\snafis>TRACERT 192.168.0.1

Tracing route to 192.168.0.1 over a maximum of 30 hops

  1   390 ms     4 ms     1 ms  192.168.0.1

Trace complete.
```

4. nbtstat

MS-DOS utility that displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP), which allow the user to troubleshoot NetBIOS name resolution issues. Normally, name resolution is done when NetBIOS over

TCP/IP is functioning correctly. It does this through local cache lookup, WINS or DNS server query or through LMHOSTS or Hosts lookup.

nbtstat syntax

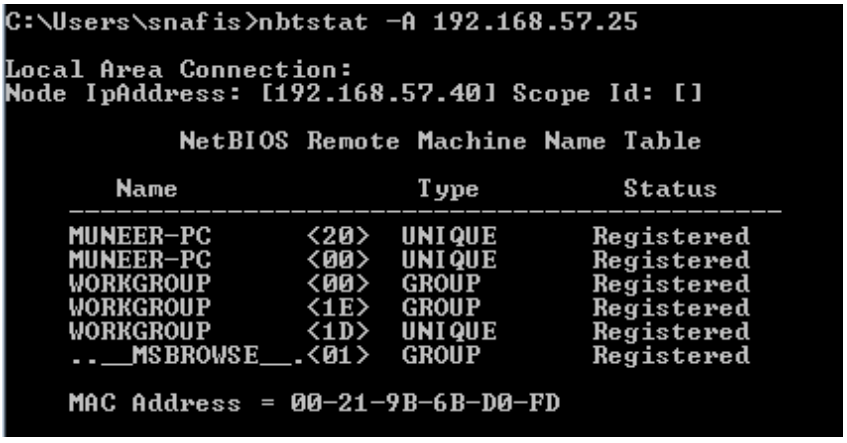
nbtstat [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]

-a	(adapter status) Lists the remote machine's name table given its name
-A	(Adapter status) Lists the remote machine's name table given its IP address.
-c	(cache) Lists NBT's cache of remote [machine] names and their IP addresses
-n	(names) Lists local NetBIOS names.
-r	(resolved) Lists names resolved by broadcast and via WINS
-R	(Reload) Purges and reloads the remote cache name table
-S	(Sessions) Lists sessions table with the destination IP addresses
-s	(sessions) Lists sessions table converting destination IP addresses to computer NETBIOS names.
-RR	(ReleaseRefresh) Sends Name Release packets to WINs and then, starts Refresh
RemoteName	Remote host machine name.
IP address	Dotted decimal representation of the IP address.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics.

nbtstat examples

nbtstat -A 204.224.150.3

The above command would run nbtstat on 204.224.150.3, a remote IP address.



5. telnet

It enables a user to telnet to another computer from the command prompt.

Telnet syntax

telnet [host [port]]

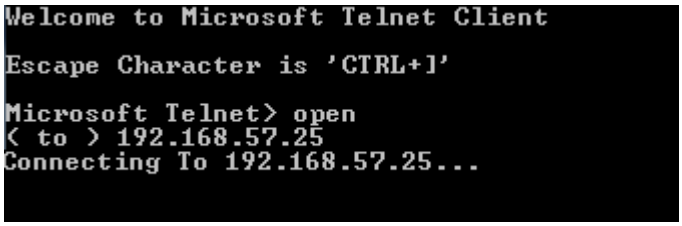
host	specifies the hostname or IP address of the remote computer.
port	Specifies the port number or service name.

Commands available through the actual telnet program:

close	close current connection
display	display operating parameters
open	connect to a site
quit	exit telnet
status	print status information
?/help	print help information

Examples

telnet 192.168.57.25



6. netstat

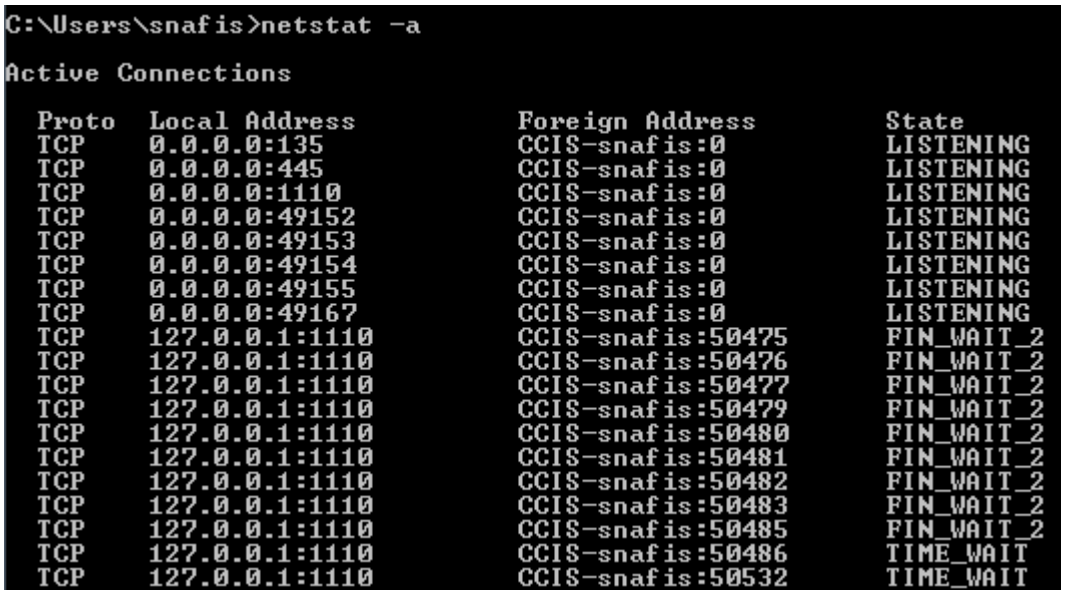
Netstat is a useful tool for checking network and Internet connections. Some useful applications for the average PC user are considered, including checking for malware connections.

Syntax and switches

Netstat syntax

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-v] [interval]

Switch	Description
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port. (Added in XP SP2.)
-e	Displays Ethernet statistics



7. tasklist

This tool displays a list of currently running processes on either a local or remote machine.

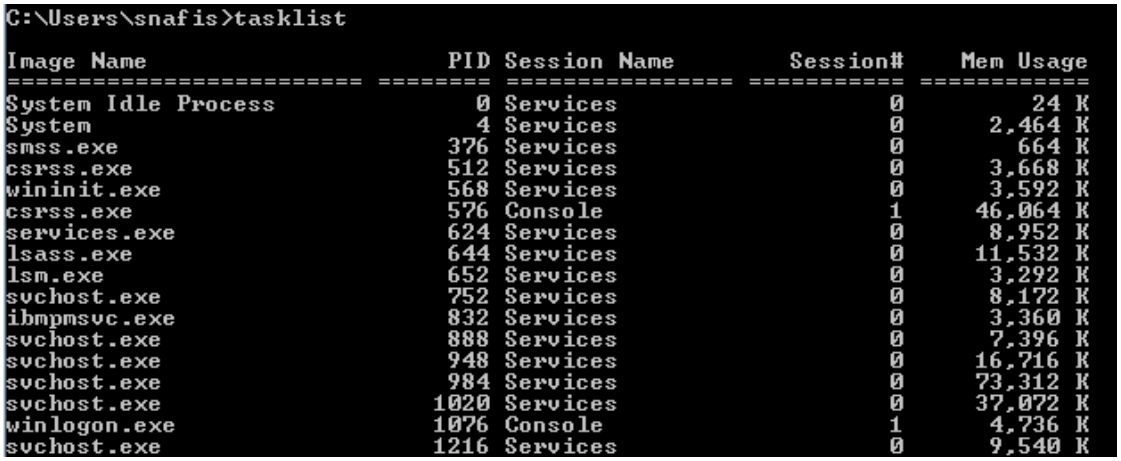
Tasklist syntax

TASKLIST [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]

Filters

/S system	Specifies the remote system to connect to.
/U [domain\]user	Specifies the user context under which the command should execute.
/P [password]	Specifies the password for the given user context. Prompts for input if omitted.
/M [module]	Lists all tasks currently using the given exe/dll name. If the module name is not specified all loaded modules are displayed.
/SVC	Displays services hosted in each process.

Example



```
C:\Users\snafis>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      2,464 K
smss.exe                       376 Services                   0        664 K
csrss.exe                      512 Services                   0      3,668 K
wininit.exe                    568 Services                   0      3,592 K
csrss.exe                      576 Console                    1     46,064 K
services.exe                   624 Services                   0      8,952 K
lsass.exe                      644 Services                   0     11,532 K
lsm.exe                        652 Services                   0      3,292 K
svchost.exe                    752 Services                   0      8,172 K
ibmpmsvc.exe                   832 Services                   0      3,360 K
svchost.exe                    888 Services                   0      7,396 K
svchost.exe                    948 Services                   0     16,716 K
svchost.exe                    984 Services                   0     73,312 K
svchost.exe                   1020 Services                   0     37,072 K
winlogon.exe                  1076 Console                    1      4,736 K
svchost.exe                   1216 Services                   0      9,540 K
```

8. getmac

It returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network.

Syntax

getmac[**.exe**] [**/s** *Computer* [**/u** *Domain\User* [**/p** *Password*]]] [**/fo** {**TABLE**|**LIST**|**CSV**}] [**/nh**] [**/v**]

Parameters

/s *Computer* : Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.

/u *Domain* \ *User* : Runs the command with the account permissions of the user specified by *User* or *Domain\User*. The default is the permissions of the current logged on user on the computer issuing the command.

/p *Password* : Specifies the password of the user account that is specified in the **/u** parameter.

/fo { TABLE | LIST | CSV } : Specifies the format to use for the query output. Valid values are **TABLE**, **LIST**, and **CSV**. The default format for output is**TABLE**.

/nh : Suppresses column header in output. Valid when the **/fo** parameter is set to **TABLE** or **CSV**.

/v : Specifies that the output display verbose information.

/? : Displays help at the command prompt.

Examples

```
C:\Users\snafis>getmac

Physical Address    Transport Name
=================== ==========================================================
80-56-F2-41-D6-04   Media disconnected
28-D2-44-32-CE-85   \Device\Tcpip_{2DE78A65-8C59-49D8-B25E-C9077860CB6B}
80-56-F2-41-D6-03   \Device\Tcpip_{A10CCBF6-05FD-45B1-BF1B-78D43F482895}
```

9. hostname

Display the hostname of the machine the command is being run on.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\snafis>hostname
CCIS-snafis

C:\Users\snafis>
```

10. pathping

Similar to the tracert command, pathping provides users with the ability of locating spots that have network latency and network loss.

Usage:

pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T] [-4] [-6] target_name

Options:

-g host-list	Loose source route along host-list.
-h maximum_hops	Maximum number of hops to search for target.
-i address	Use the specified source address.
-n	Do not resolve addresses to hostnames.
-p period	Wait period milliseconds between pings.
-q num_queries	Number of queries per hop.
-w timeout	Wait timeout milliseconds for each reply.
-P	Test for RSVP PATH connectivity.
-R	Test if each hop is RSVP aware.
-T	Test connectivity to each hop with Layer-2 priority tags.
-4	Force using IPv4.
-6	Force using IPv6.

```
C:\Users\snafis>pathping 192.168.57.25

Tracing route to MUNEER-PC [192.168.57.25]
over a maximum of 30 hops:
  0  CCIS-snafis.jazanu.edu.sa [192.168.57.40]
  1  MUNEER-PC [192.168.57.25]

Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           CCIS-snafis.jazanu.edu.sa [192.168
.57.40]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  MUNEER-PC [192.168.57.25]

Trace complete.
```

11. route

Command to show or manually configure the routes in the routing table.

Syntax

ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

-f	Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.
-p	When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. When used with the PRINT command, displays the list of registered persistent routes. Ignored for all other commands, which always affect the appropriate persistent routes. This option is not supported Windows'95. Command
-4	Force using IPv4.
-6	Force using IPv6.
command	One of these: PRINT Prints a route ADD Adds a route DELETE Deletes a route CHANGE Modifies an existing route destination
destination	Specifies the host.
MASK	Specifies that the next parameter is the 'netmask' value.
netmask	Specifies a subnet mask value for this route entry. If not specified, it defaults to 255.255.255.255.
gateway	Specifies gateway.
interface	the interface number for the specified route.
METRIC	Specifies the metric, ie. cost for the destination.

```
C:\Users\snafis>route PRINT
===========================================================================
Interface List
 14...80 56 f2 41 d6 03 ......2x2 11b/g/n Wireless LAN M.2 Adapter
 13...28 d2 44 32 ce 85 ......Intel(R) Ethernet Connection I217-LM
 12...80 56 f2 41 d6 04 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
 19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
 20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
 35...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #7
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.0.1    192.168.0.104     20
          0.0.0.0          0.0.0.0     192.168.57.1   192.168.57.40     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.0.0    255.255.255.0         On-link     192.168.0.104    276
    192.168.0.104  255.255.255.255         On-link     192.168.0.104    276
    192.168.0.255  255.255.255.255         On-link     192.168.0.104    276
     192.168.57.0    255.255.255.0         On-link     192.168.57.40    266
    192.168.57.40  255.255.255.255         On-link     192.168.57.40    266
   192.168.57.255  255.255.255.255         On-link     192.168.57.40    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.57.40    266
        224.0.0.0        240.0.0.0         On-link     192.168.0.104    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.57.40    266
  255.255.255.255  255.255.255.255         On-link     192.168.0.104    276
===========================================================================
Persistent Routes:
  None
```

12. fc

FC, or file compare, is used to compare two files against each other. Once completed, fc returns lines that differ between the two files. If no lines differ, you will receive a message indicating no differences encountered.

fc syntax

Compares two files or sets of files and displays the differences between them.

FC [/A] [/C] [/L] [/LBn] [/N] [/T] [/W] [/nnnn] [drive1:][path1]filename1 [drive2:][path2]filename2

FC /B [drive1:][path1]filename1 [drive2:][path2]filename2

/A	Displays only first and last lines for each set of differences.
/B	Performs a binary comparison.
/C	Disregards the case of letters.
/L	Compares files as ASCII text.
/LBn	Sets the maximum consecutive mismatches to the specified number of lines.
/N	Displays the line numbers on an ASCII comparison.
/T	Does not expand tabs to spaces.

/W	Compresses white space (tabs and spaces) for comparison.
/nnnn	Specifies the number of consecutive lines that must match after a mismatch.
[drive1:][path1]filename1	Specifies the first file or set of files to compare.
[drive2:][path2]filename2	Specifies the second file or set of files to compare.

fc examples

fc autoexec.bat config.sys

13. sfc

Scan System Files for Problems. Short for **System File Checker, SFC** is a command that scans and replaces any Microsoft Windows file on the computer and replaces any changed file with the correct version. This is a great command to run when you are running into an issue that is difficult to troubleshoot.

syntax

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>] [/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory>]

/SCANNOW	Scans integrity of all protected system files and repairs files with problems when possible.
/VERIFYONLY	Scans integrity of all protected system files. No repair operation is performed.
/SCANFILE	Scans integrity of the referenced file, repairs file if problems are identified. Specify full path <file>.
/VERIFYFILE	Verifies the integrity of the file with full path <file>. No re pair operation is performed.
/OFFBOOTDIR	For offline repair specify the location of the offline boot directory.
/OFFWINDIR	For offline repair specify the location of the offline Windows directory.

14. recimg

Create custom recovery images. It is one of hidden feature of creating custom recovery images. Using this command, you can create your custom recovery images. Using this feature, you can remove default bloatware and also enables you to add your favourite third party programs to recovery images to your PC easily.

15. cipher

Displays or alters the encryption of directories [files] on NTFS partitions.

Syntax

CIPHER [/E | /D | /C] [/S:directory] [/B] [/H] [pathname [...]]

CIPHER /K [/ECC:256|384|521]

CIPHER /R:filename [/SMARTCARD] [/ECC:256|384|521]

CIPHER /U [/N]

CIPHER /W:directory

CIPHER /X[:efsfile] [filename]

CIPHER /Y

CIPHER /ADDUSER [/CERTHASH:hash | /CERTFILE:filename | /USER:username] [/S:directory] [/B] [/H] [pathname [...]]

CIPHER /FLUSHCACHE [/SERVER:servername]

CIPHER /REMOVEUSER /CERTHASH:hash [/S:directory] [/B] [/H] [pathname [...]]

CIPHER /REKEY [pathname [...]]

/B	Abort if an error is encountered. By default, CIPHER continues executing even if errors are encountered.
/C	Displays information on the encrypted file.
/D	Decrypts the specified directories. Directories will be marked so that files added afterward will not be encrypted.
/E	/E Encrypts the specified files or directories. Directories will be marked so that files added afterward will be encrypted. The encrypted file could become decrypted when it is modified if the parent directory is not encrypted. It is recommended that you encrypt the file and the parent directory.
/H	Displays files with the hidden or system attributes. These files are omitted by default.
/K	Create new file encryption key for the user running CIPHER. If this option is chosen, all the other options will be ignored. Note: By default, /K creates a certificate and key that conform to current group policy. If ECC is specified, a self-signed certificate will be created with the supplied key size.
/N	This option only works with /U and prevents keys being updated. This is used to find all the encrypted files on the local drives.
/R	/R Generates an EFS recovery key and certificate, then writes them to a .PFX file (containing certificate and private key) and a .CER

	file (containing only the certificate). An administrator may add the contents of the .CER to the EFS recovery policy to create the recovery key for users, and import the .PFX to recover individual files. If SMARTCARD is specified, then writes the recovery key and certificate to a smart card. A .CER file is generated (containing only the certificate). No .PFX file is generated. Note: By default, /R creates an 2048-bit RSA recovery key and certificate. If ECC is specified, it must be followed by a key size of 256, 384, or 521.
/S	Performs the specified operation on directories in the given directory and all subdirectories.
/U	Tries to touch all the encrypted files on local drives. The /U switch update user's file encryption key or recovery keys to the current ones if they are changed. This option does not work with other options except /N.
/W	Removes data from available unused disk space on the entire volume. If this option is chosen, all other options are ignored. The directory specified can be anywhere in a local volume. If it is a mount point or points to a directory in another volume, the data on that volume will be removed.
/X	Backup EFS certificate and keys into file filename. If efsfile is provided, the current user's certificate(s) used to encrypt the file will be backed up. Otherwise, the user's current EFS certificate and keys will be backed up.
/Y	Displays your current EFS certificate thumbprint on the local PC.
/ADDUSER	Adds a user to the specified encrypted file(s). If CERTHASH is provided, cipher will search for a certificate with this SHA1 hash. If CERTFILE is provided, cipher will extract the certificate from the file. If USER is provided, cipher will try to locate the user's certificate in Active Directory Domain Services.
/FLUSHCACHE	Clears the calling user's EFS key cache on the specified server. If servername is not provided, cipher clears the user's key cache on the local machine.
/REKEY	Updates the specified encrypted file(s) to use the configured EFS current key.
/REMOVEUSER	Removes a user from the specified file(s). CERTHASH must be the SHA1 hash of the certificate to remove.
directory	A directory path.
filename	A filename without extensions.
pathname	Specifies a pattern, file or directory.
efsfile	An encrypted file path.

16. arp

Displays, adds, and removes arp information from network devices.

ARP -s inet_addr eth_adr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
-g	Same as –a
inet_addr	Specifies an Internet address.
-N if addr	Displays the ARP entries for the network interface specified by if_addr.
-d	Deletes the host specified by inet_addr.
-s	Adds the host and associates the Internet address inet_addr with the physical address eth_addr. The physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr	Specifies a physical address
if_addr	If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

ARP examples : arp –a

```
C:\Users\snafis>arp -a

Interface: 192.168.57.40 --- 0xd
  Internet Address      Physical Address      Type
  192.168.57.1          44-2b-03-e0-b0-00     dynamic
  192.168.57.25         00-21-9b-6b-d0-fd     dynamic
  192.168.57.33         00-21-9b-67-9d-7d     dynamic
  192.168.57.37         f0-de-f1-1c-f2-09     dynamic
  192.168.57.43         00-21-9b-32-5c-5f     dynamic
  192.168.57.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.104 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1           e8-94-f6-c5-bf-00     dynamic
  192.168.0.100         18-3d-a2-90-11-70     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  238.255.255.0         01-00-5e-7f-ff-00     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

17. net view

It displays a list of computers in a specified workgroup or the shared resources available on a specified computer.

Syntax:

[\\computername [/CACHE] | /DOMAIN[:domainname]]

NET VIEW /NETWORK:NW [\\computername]