CySA+ Lab Series

Lab 03: Windows CLI Tools

Document Version: 2022-10-10

Material in this Lab Aligns to the Following	
CompTIA CySA+ (CS0-002) Exam Objectives	1.4 - Given a scenario, analyze the output from common vulnerability tools 2.1 - Explain software assurance best practices
All-In-One CompTIA CySA+ Second Edition ISBN-13: 978-1260464306 Chapters	4: Vulnerability Assessment Tools 9: Software Assurance Best Practices

Contents

Introduction

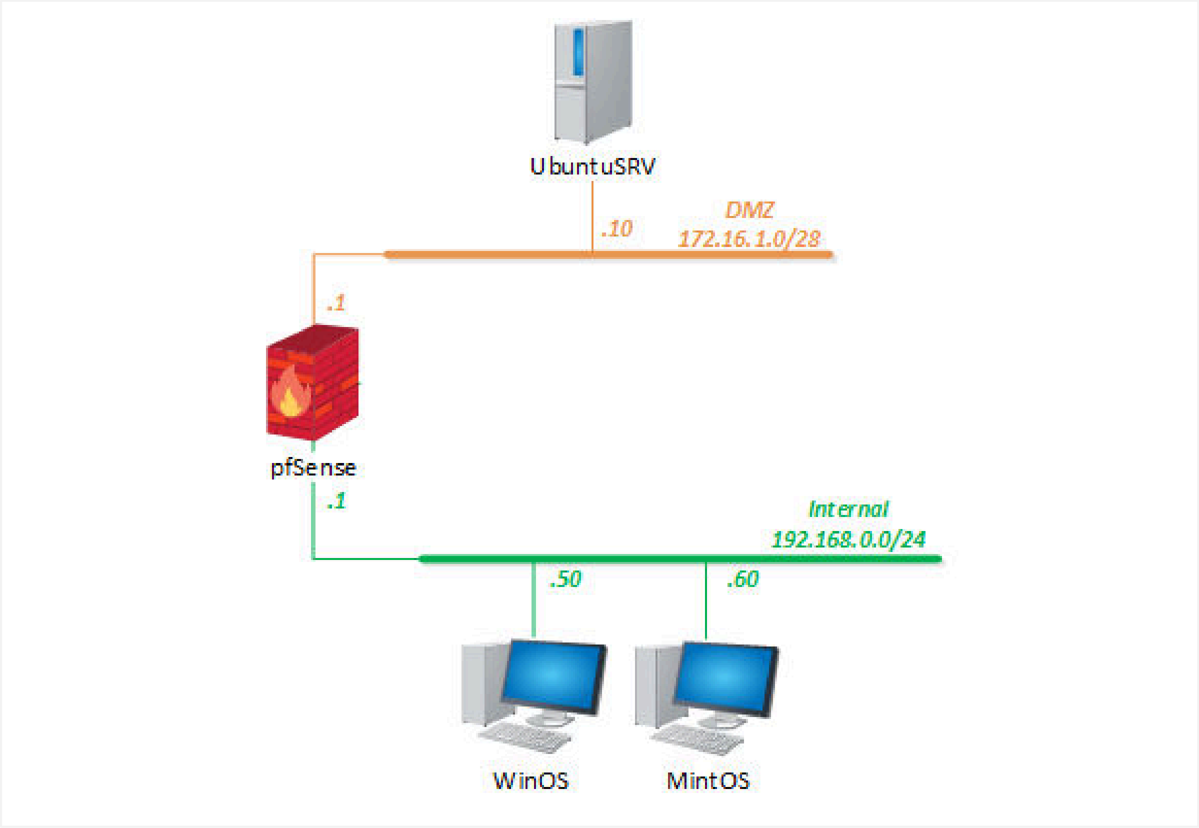
There are many tools that are included with the Windows operating systems that will assist in cybersecurity analysis.

Objective

In this lab, you will explore various Windows command line tools to understand the services and processes running on the Windows system.

- Using *IPCONFIG*
- Using *PING*
- Using *WHOAMI*
- Identifying Routes
- Identifying User and Nearby Systems Using ARP

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

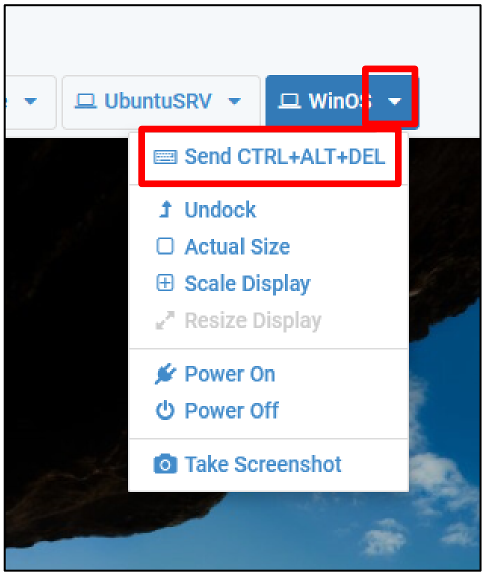
Virtual Machine	IP Address	Account	Password
WinOS (Server 2019)	`192.168.0.50`	`Administrator`	`NDGlabpass123!`
MintOS (Linux Mint)	`192.168.0.60`	`sysadmin`	`NDGlabpass123!`
OSSIM (Alien Vault)	`172.16.1.2`	`root`	`NDGlabpass123!`
UbuntuSRV (Ubuntu Server)	`172.16.1.10`	`sysadmin`	`NDGlabpass123!`
Kali	`203.0.113.2`	`sysadmin`	`NDGlabpass123!`

pfSense	`203.0.113.1`
	`172.16.1.1`
	`192.168.0.1`
		`admin`	`NDGlabpass123!`

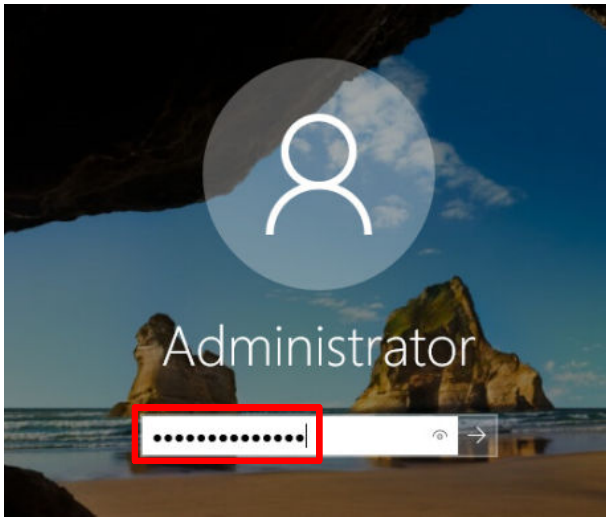
1 Using IPCONFIG

IPCONFIG is a Windows console application that displays information about the IPv4 and IPv6 stack on a Windows computer. It can also be used to reset DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name Service). The command and options are the same on all past and present versions of Windows.

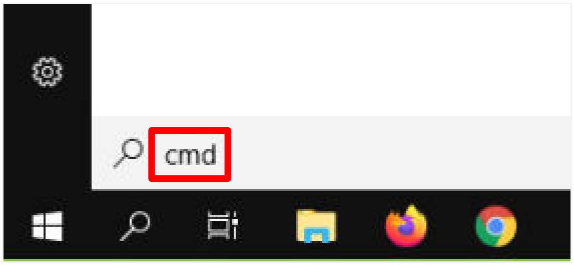
1. Set the focus to the **WinOS** computer.
2. Bring up the login window by sending a Ctrl + Alt + Delete. To do this, click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



3. Log in as *Administrator* using the password: `NDGlabpass123!`

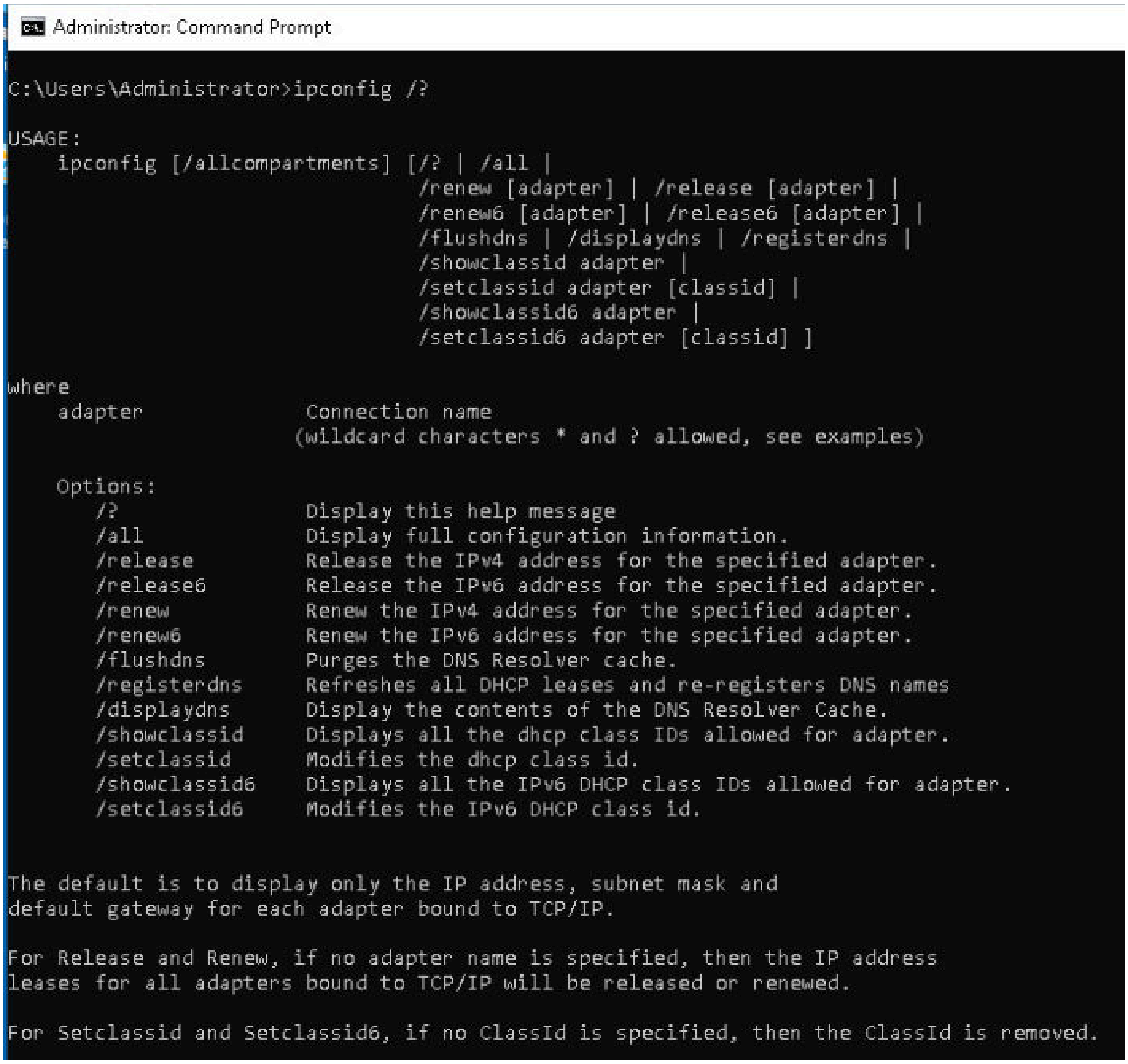


4. Click on the **Windows Start** button in the bottom-left corner, type `cmd`, and then press the **Enter** key to bring up the command prompt window.



5. In the command prompt window, type the following command to show the *ipconfig* help screen.

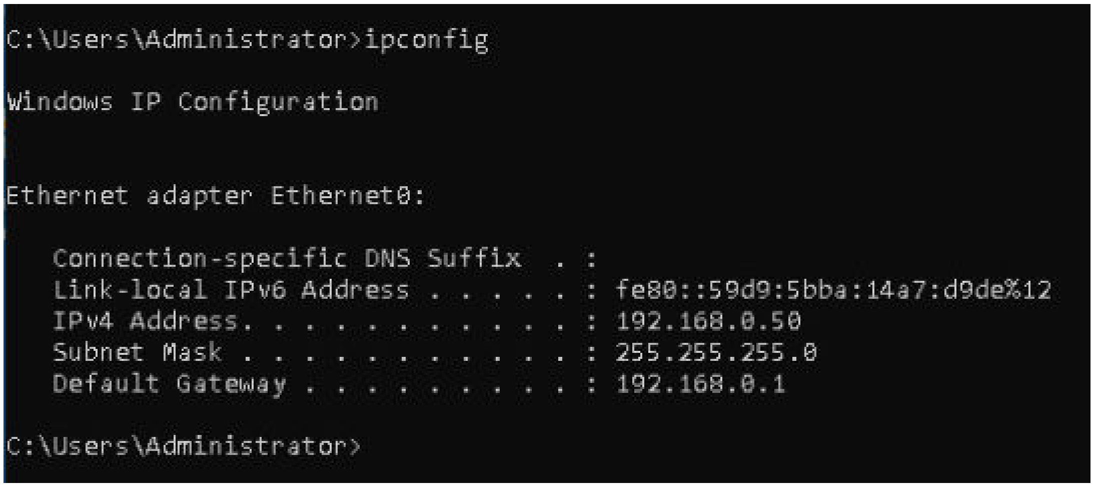
```
ipconfig /?
```



```
C:\Users\Administrator>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.
```

6. To show the *IP Address, Subnet Mask,* and *Default Gateway* for all the adapters, type the following command:

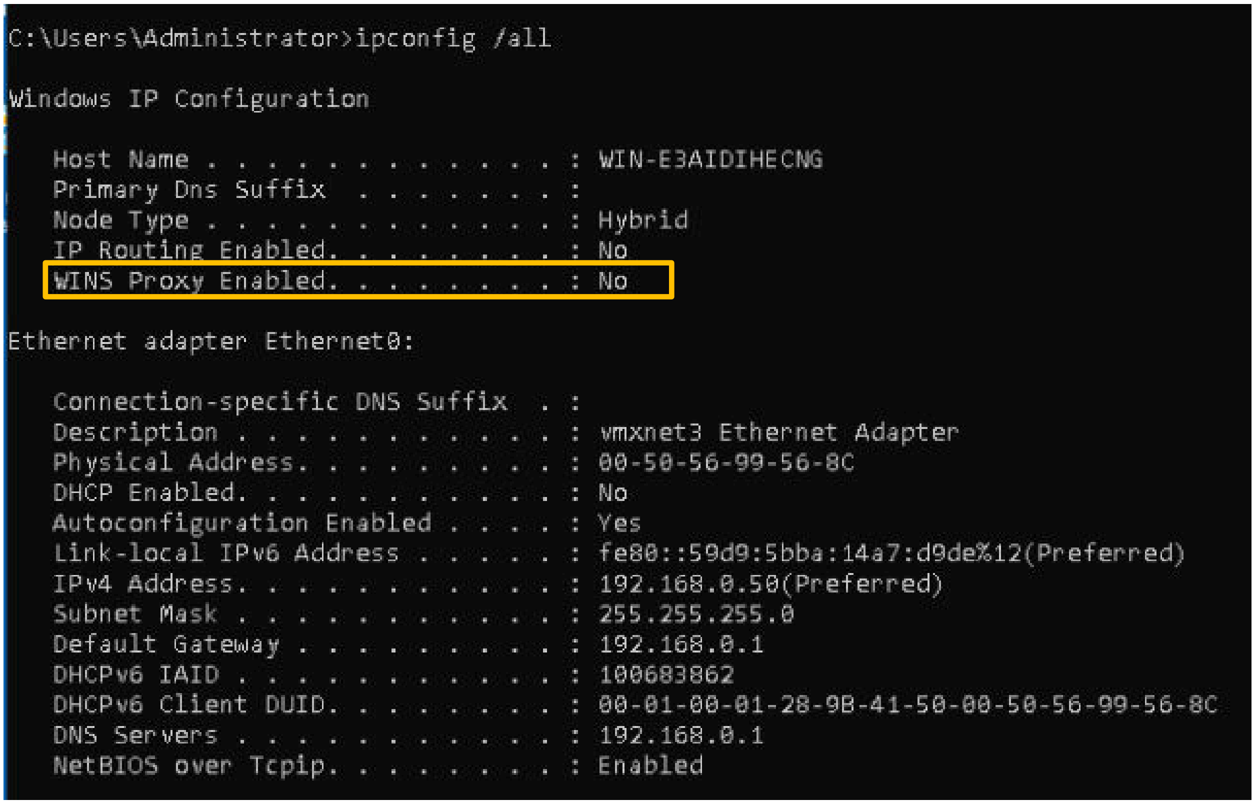
```
ipconfig
```



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::59d9:5bba:14a7:d9de%12
   IPv4 Address. . . . . . . . . . . : 192.168.0.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\Administrator>
```

7. To show the full TCP/IP stack, including the *Host Name, MAC Address, DNS Servers*, and if the address was supplied by *DHCP*, type the following command:

```
ipconfig /all
```

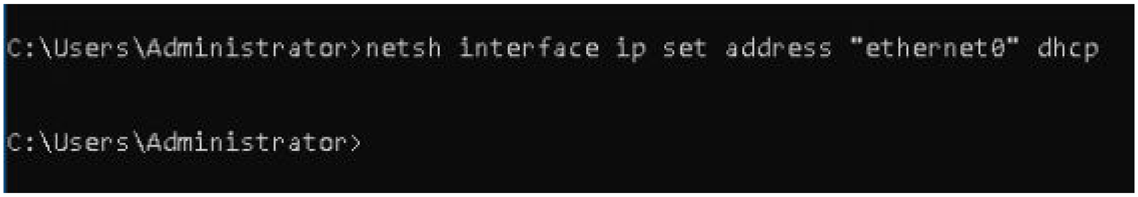


```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-E3AIDIHECNG
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-99-56-8C
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::59d9:5bba:14a7:d9de%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.50(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 100683862
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-9B-41-50-00-50-56-99-56-8C
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

If you look at the **DHCP Enabled** entry on the **ipconfig /all** screen, you will see that DHCP is not enabled, which means that the IP address is manually configured to use a static IP address.

8. To perform the remaining steps in the lab, DHCP will need to be enabled. In the command prompt window, type the following command to change the adapter's IP:

```
netsh interface ip set address "ethernet0" dhcp
```



```
C:\Users\Administrator>netsh interface ip set address "ethernet0" dhcp

C:\Users\Administrator>
```

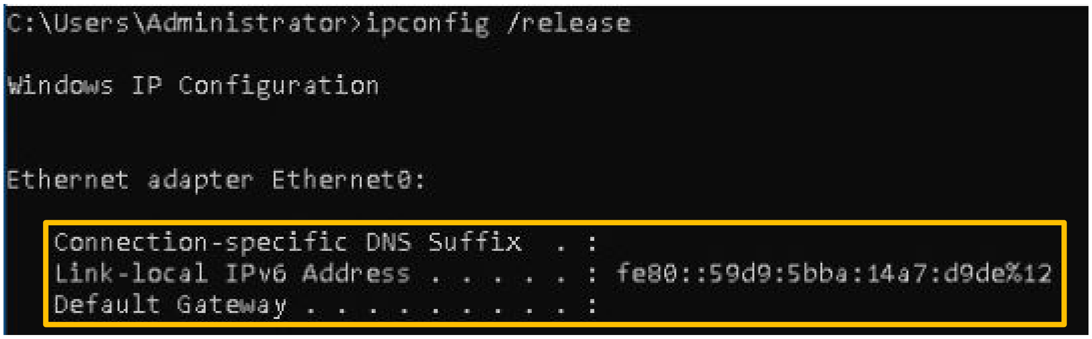
If the command executed correctly, you will not get any reply message.

The most common way to change the IP address stack uses the Windows 10 Settings app or the Control Panel. The command line method is used less, but it is more efficient.

9. If the Windows computer leased an IP address through a DHCP server, the following command would release the address' lease:

```
ipconfig /release
```

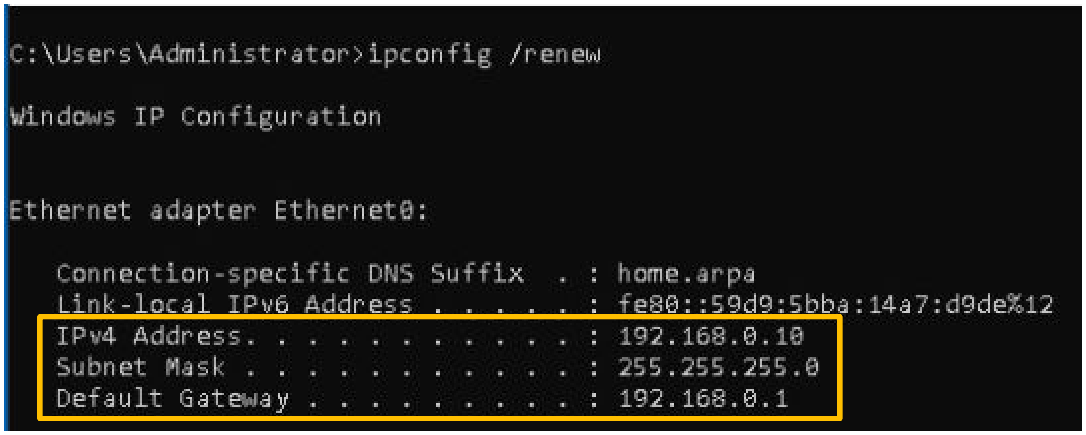
You can see that there is no IP address and default gateway.



```
C:\Users\Administrator>ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::59d9:5bba:14a7:d9de%12
   Default Gateway . . . . . . . . . :
```

10. To renew the DHCP address lease, type the following command:

```
ipconfig /renew
```



```
C:\Users\Administrator>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home.arpa
   Link-local IPv6 Address . . . . . : fe80::59d9:5bba:14a7:d9de%12
   IPv4 Address. . . . . . . . . . . : 192.168.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

11. Leave the *WinOS* machine open and continue to the next task.

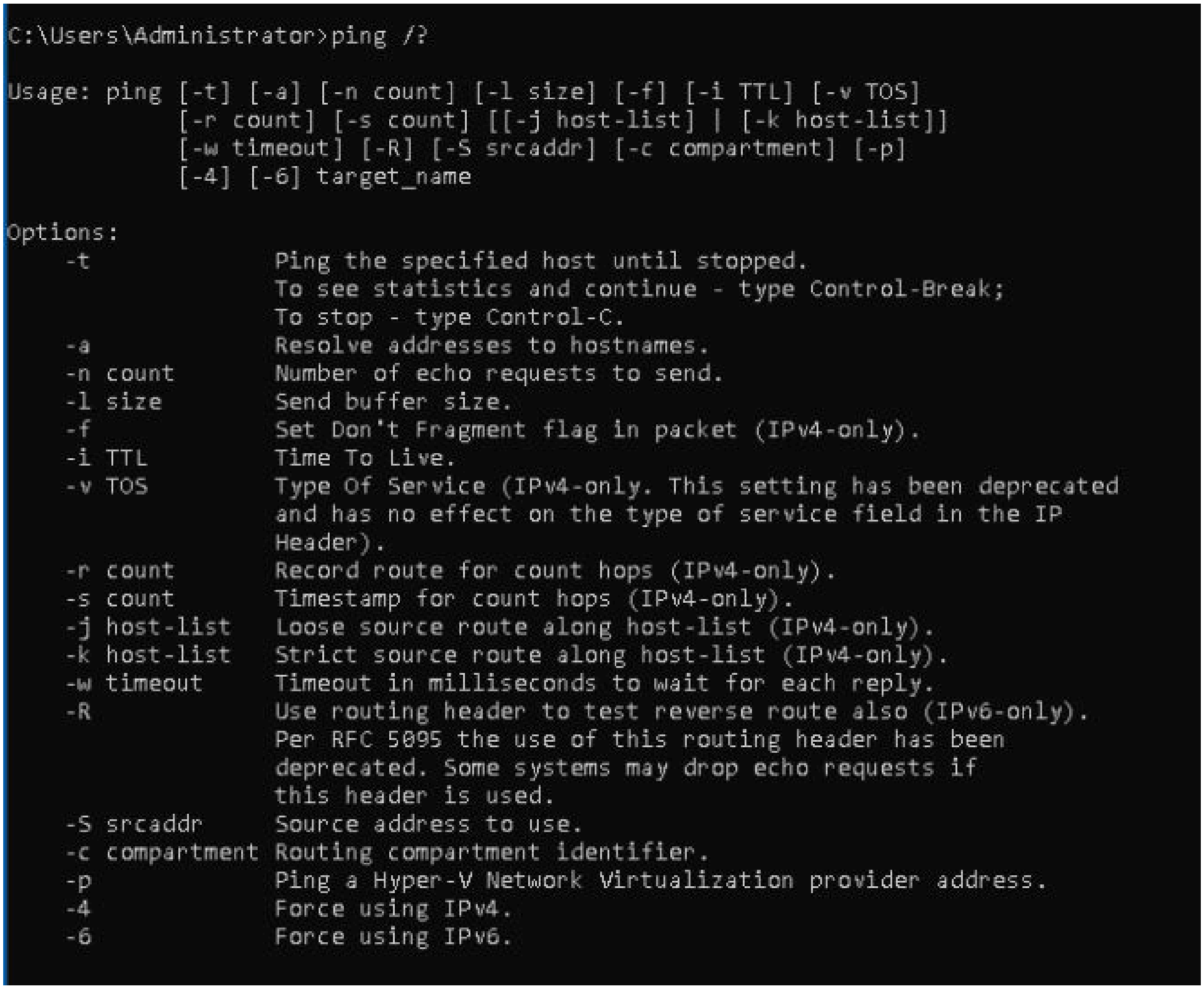
2 Using PING

The ping command is used to verify network level connectivity between hosts by sending out an ICMP (Internet Control Message Protocol) Echo Request packet to the other hosts' IP address which then returns an ICMP Echo Reply packet. The results of the reply are displayed on the console screen. Part of the reply contains information about how long it takes for the round trip, which can inform you about your network's latency time.

The ping command is a TCP/IP command and can be used on many different operating systems, including Windows, macOS, and Linux/Unix. It is used to troubleshoot connectivity, reachability, and name resolution issues. You can ping a host by IP address or by hostname. If you can ping a host by IP address but not by name, you know you have a problem with name resolution using DNS (Domain Name System) or the local HOSTS file (Windows hosts can resolve names using NetBIOS).

1. In the command prompt window, type the following command to show the *ping* help screen.

```
ping /?
```

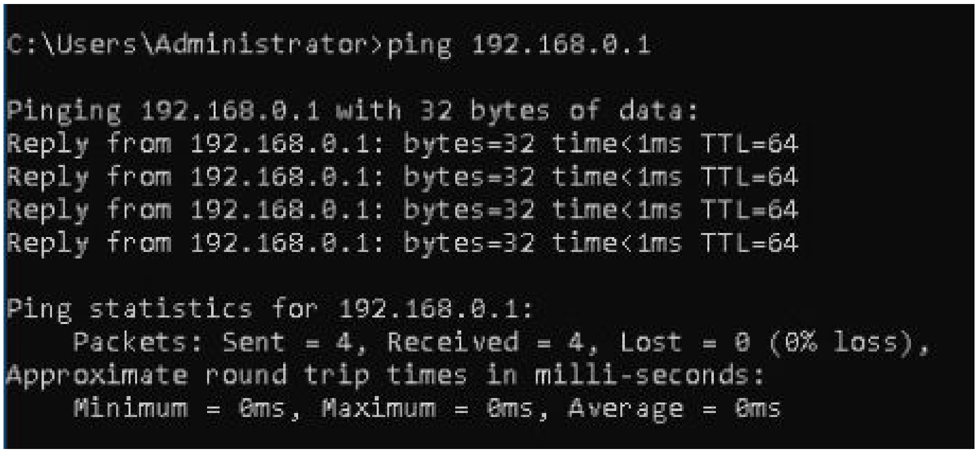


```
C:\Users\Administrator>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

2. To execute the basic *ping* command, type the following command:

```
ping 192.168.0.1
```

By default, the *ping* command will send out four **ICMP Echo Requests** and will display the reply for each one. An important value to look at is the **Approximate Round Trip Times in Milliseconds**. This can be used to determine latency which can be useful in troubleshooting connectivity.



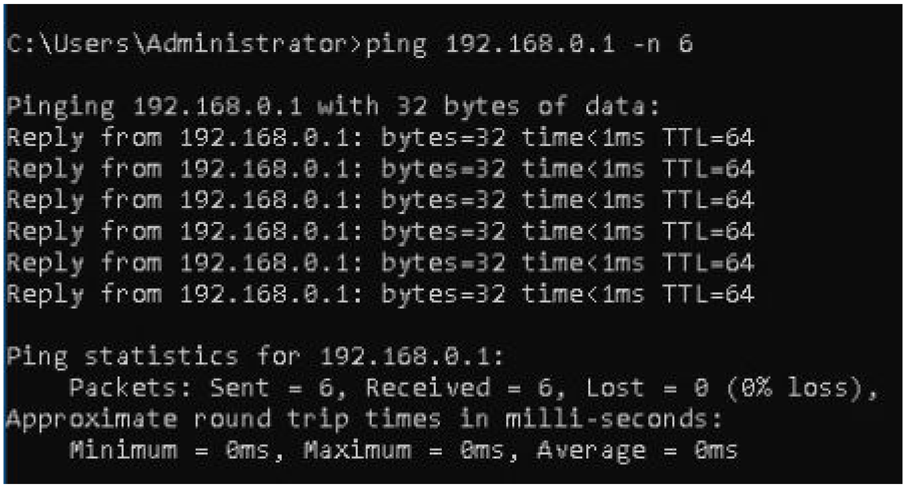
```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In Windows, the *ping* command, by default, sends four ping requests.

In macOS and Unix/Linux, the *ping* command will send continuous pings until the user stops it.

3. You can specify how many pings to send by using the **–n <*count number*>** option.

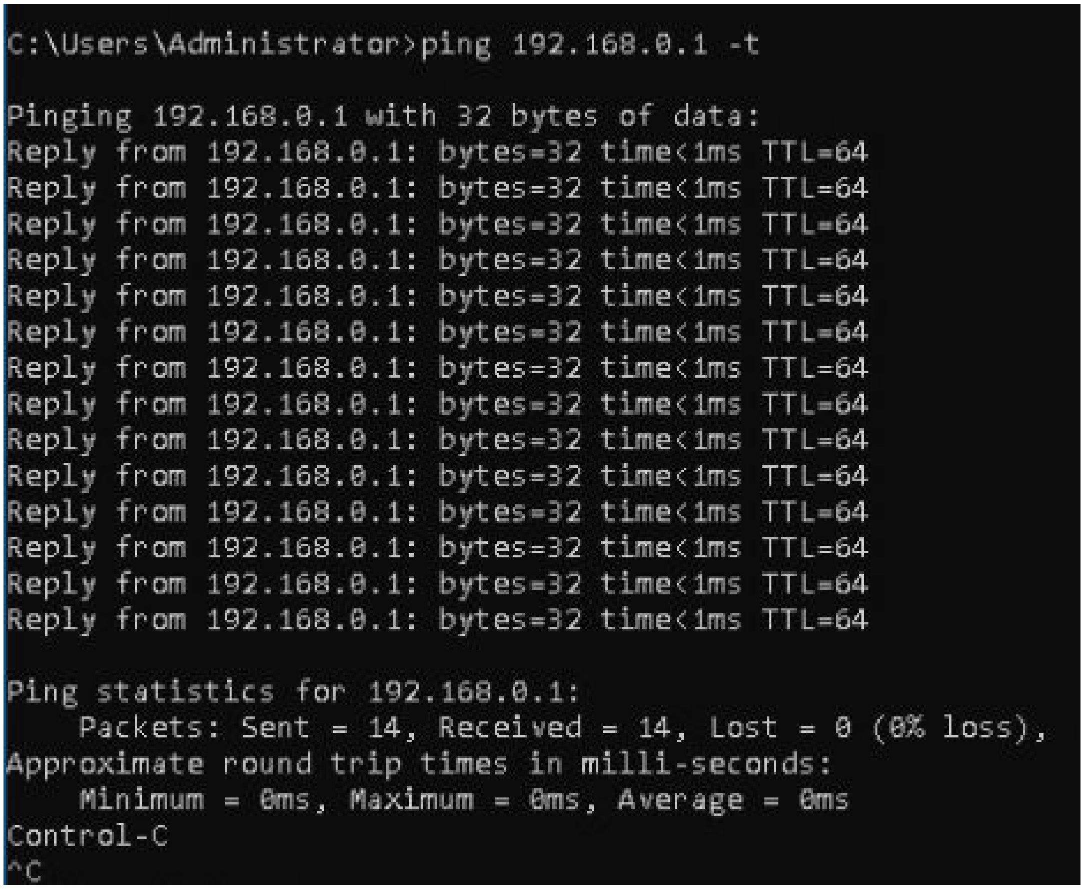
```
ping 192.168.0.1 –n 6
```



```
C:\Users\Administrator>ping 192.168.0.1 -n 6

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4. To have a host send pings continuously, there is the **–t** option that will send out *ICMP Echo Requests* until you manually stop the process by pressing **CTRL+C**.

```
ping 192.168.0.1 –t
```



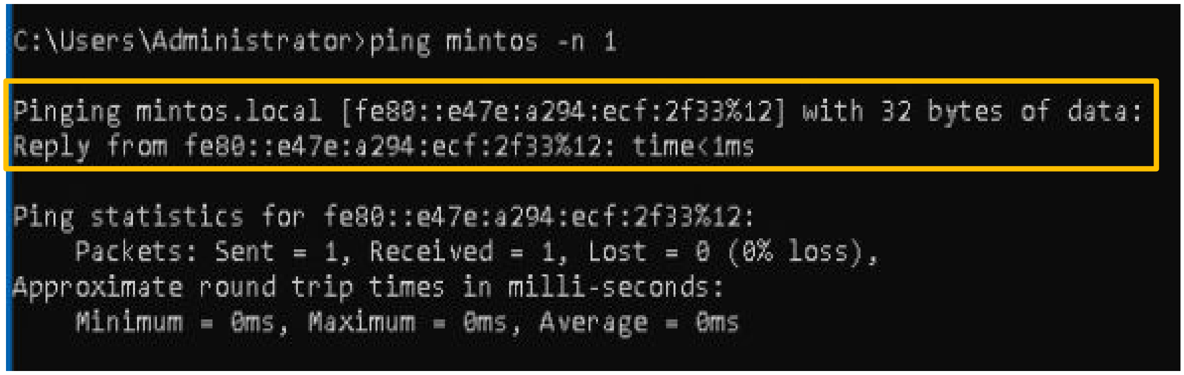
```
C:\Users\Administrator>ping 192.168.0.1 -t

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 14, Received = 14, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
```

To end the continuous ping, press **CTRL+C.**

5. If you want to send a single ping to a host by name, type the following command:

```
ping mintos –n 1
```

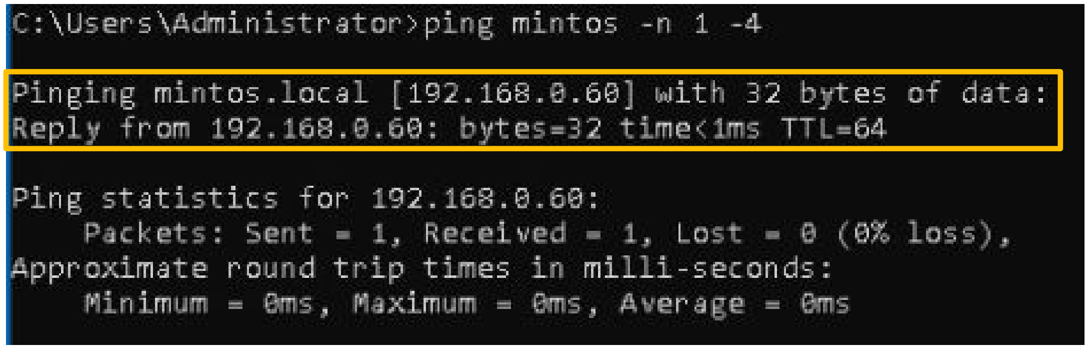
By default, when you ping a hostname, the reply will show the IPv6 address.



```
C:\Users\Administrator>ping mintos -n 1

Pinging mintos.local [fe80::e47e:a294:ecf:2f33%12] with 32 bytes of data:
Reply from fe80::e47e:a294:ecf:2f33%12: time<1ms

Ping statistics for fe80::e47e:a294:ecf:2f33%12:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6. Add the **-4** option to show the IPv4 address.

```
ping mintos -n 1 -4
```



```
C:\Users\Administrator>ping mintos -n 1 -4

Pinging mintos.local [192.168.0.60] with 32 bytes of data:
Reply from 192.168.0.60: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.60:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

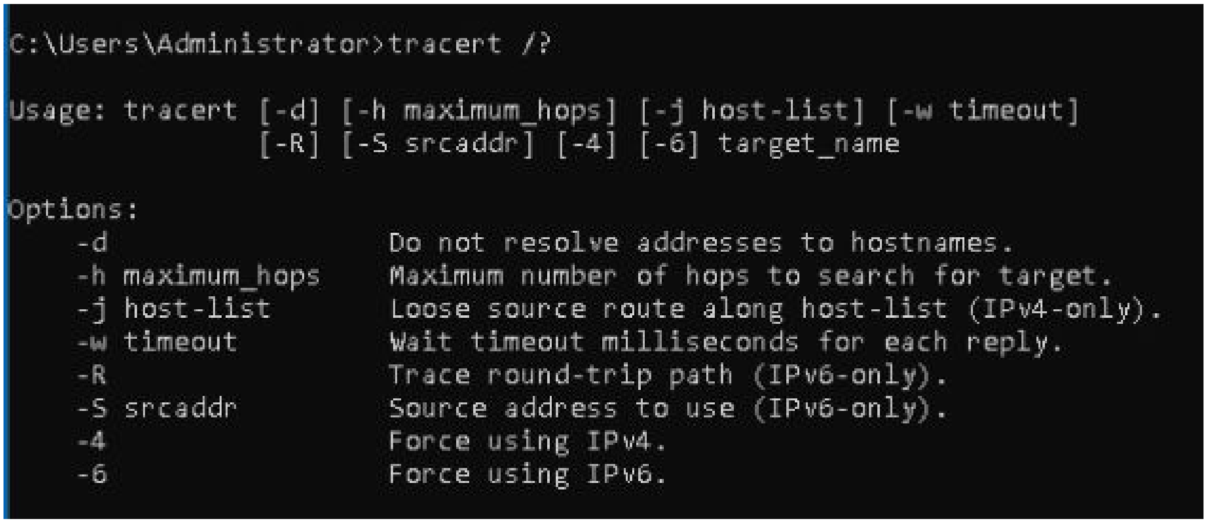
7. Leave the *WinOS* machine open and continue to the next task.

3 Using TRACERT

The *tracert* command is used to determine the path that is taken to reach a destination host address. It uses a succession of **ICMP Echo Request** (ping) packets with modified TTL values to determine the IP address and name for each router and network that the ping packets traverse.

1. In the command prompt window, type the following command to show the *tracert* help screen.

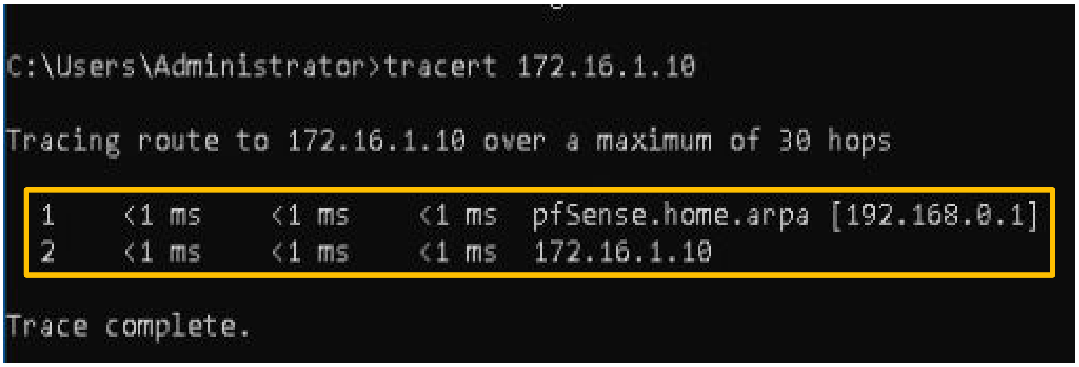
```
tracert /?
```



```
C:\Users\Administrator>tracert /?

Usage: 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.
    -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.
```

2. Let's test it out by sending a **tracert** command to the *UbuntuSRV* host at **172.16.1.10** by typing the following command:

```
tracert 172.16.1.10
```



```
C:\Users\Administrator>tracert 172.16.1.10

Tracing route to 172.16.1.10 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  pfSense.home.arpa [192.168.0.1]
  2    <1 ms    <1 ms    <1 ms  172.16.1.10

Trace complete.
```

In the *tracert* output, each row you see indicates when the packet crosses a router or terminates at the host IP address. There are three columns (*tracert* sends three packets) that show the **Round Trip Time** (**RTT**) that it took for the packet to reach the router and return.

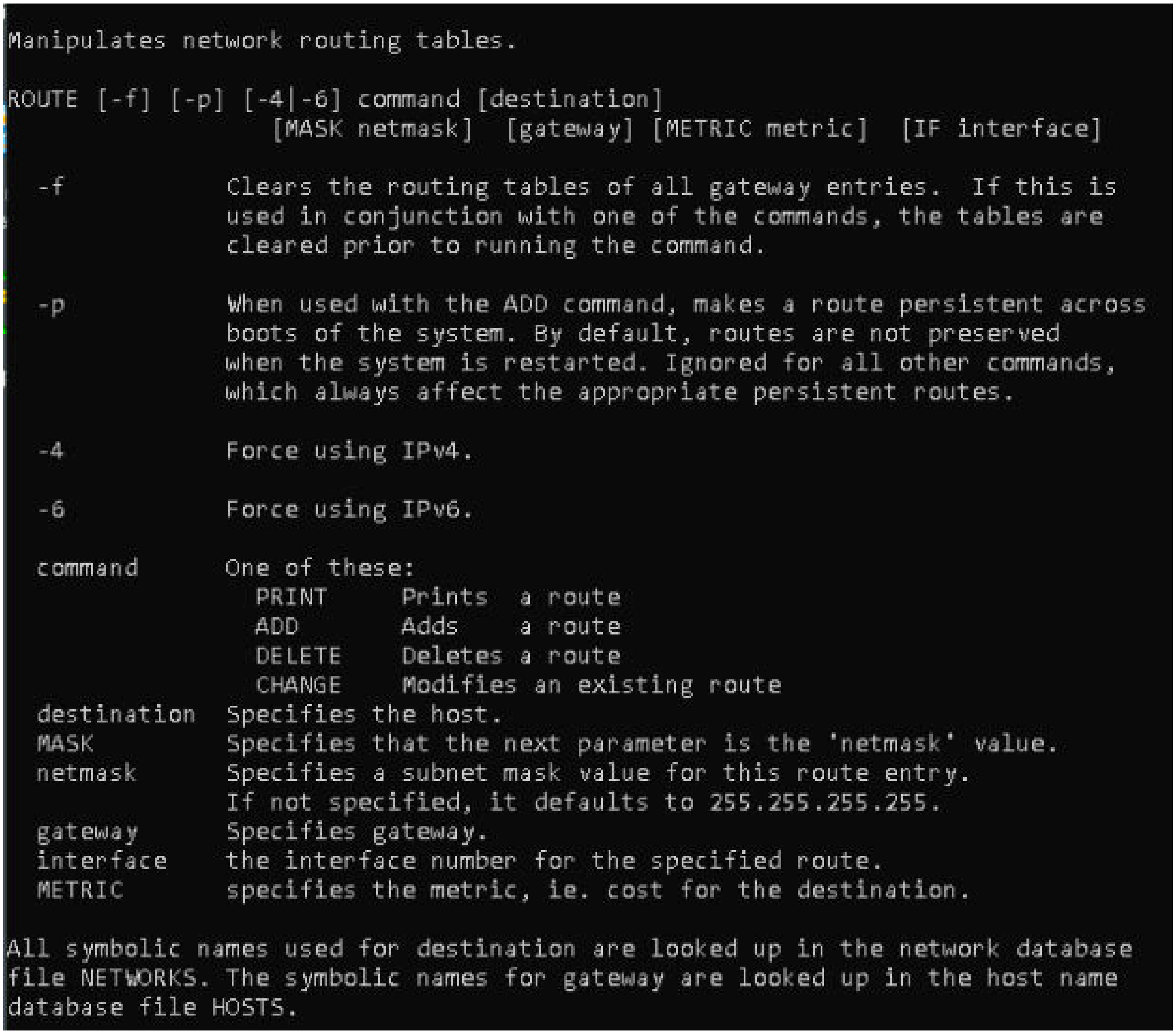
3. Leave the *WinOS* machine open and continue to the next task.

4 Using ROUTE

The *route* command displays and can allow modification to the routing table on the local host. Without any optional switches or parameters, the *route* command will display just the help screen.

1. In the command prompt window, type the following command to show the *route* help screen.

```
route
```



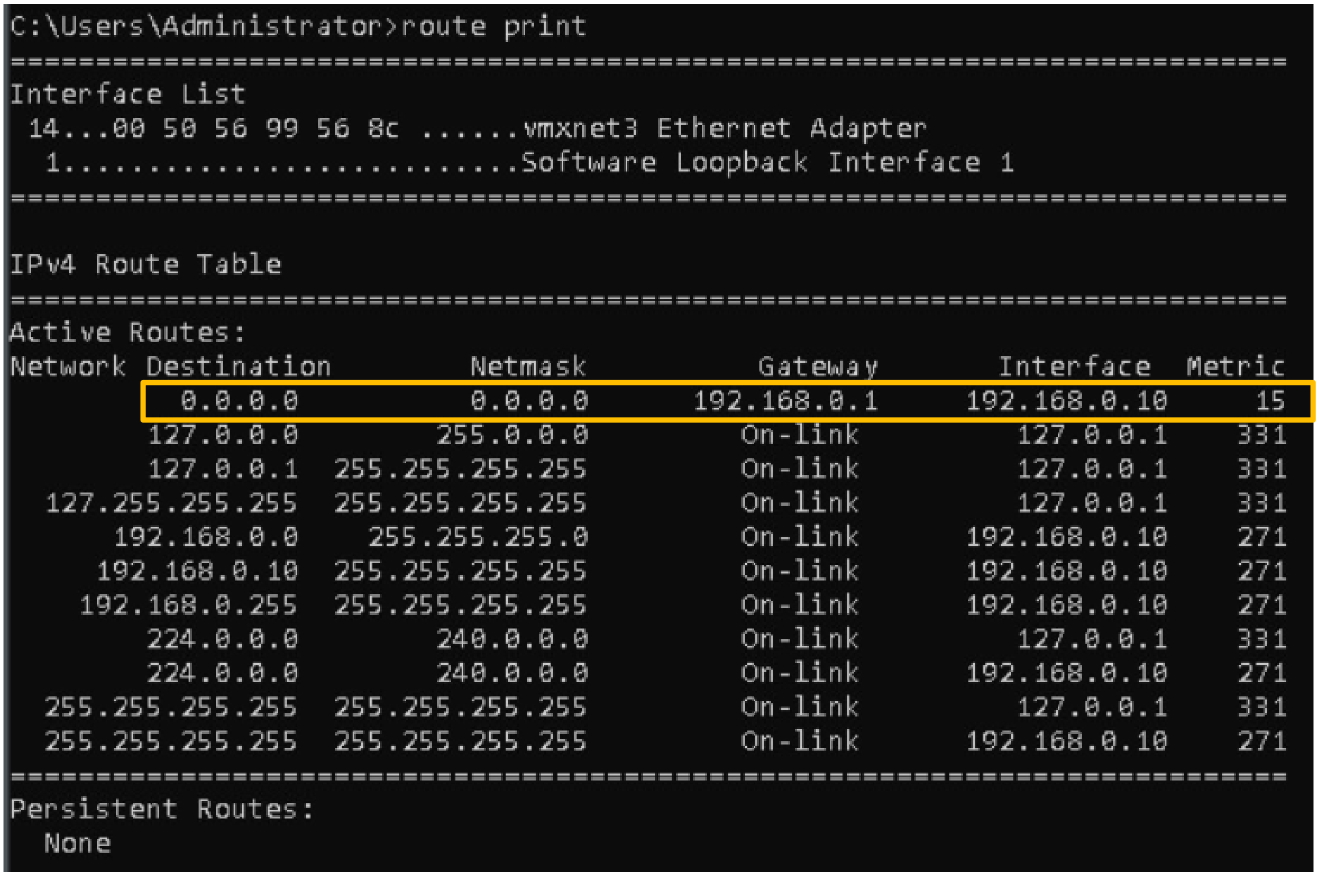
```
Manipulates network routing tables.

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. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -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  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.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.
```

2. The *route* command has several options. The four commands that are used are **add** [adds a route], **change** [modifies an existing route], **delete** [deletes a route], and **print** [displays the routing table]. To display the contents of the routing table, type the following command:

```
route print
```

The columns in the routing table are:

Network Destination	The Network IP address of a remote network.
Netmask	The network or subnet mask, shown in dotted notation.
Gateway	The IP address of the default gateway, or the "next hop" to direct the packet off to the router, which will route the packet to the next network. The "On-link" entry means the destination network is directly attached to the Window computer's interface.
Interface	The IP address of the Window's computer NIC. 127.0.0.1 is the loopback address of the interface.
Metric	The Administrative Distance or Cost to the destination network. If there are multiple routes to the same destination, the one with the lowest metric is chosen.



```
C:\Users\Administrator>route print
===========================================================================
Interface List
 14...00 50 56 99 56 8c ......vmxnet3 Ethernet Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.10     15
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link      192.168.0.10    271
     192.168.0.10  255.255.255.255         On-link      192.168.0.10    271
    192.168.0.255  255.255.255.255         On-link      192.168.0.10    271
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.0.10    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.0.10    271
===========================================================================
Persistent Routes:
  None
```

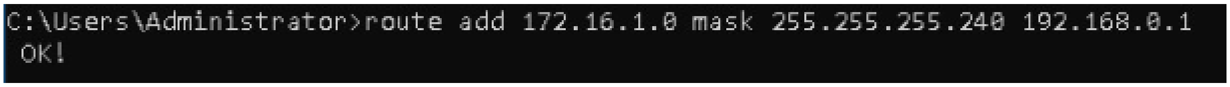
The **0.0.0.0 Network Destination** shows the **Default Gateway**, which is the next hop address if there are no other destination matches in the routing table.

3. To add a route in the routing table, the syntax is:

   route add <*destination network*> mask <*destination network subnet mask*> <*gateway IP*>

   Type the following command to add a new route entry to the DMZ network (172.16.1.0/28):

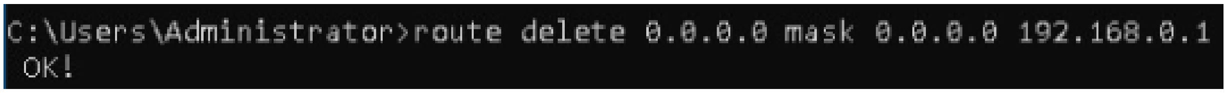
```
route add 172.16.1.0 mask 255.255.255.240 192.168.0.1
```



```
C:\Users\Administrator>route add 172.16.1.0 mask 255.255.255.240 192.168.0.1
 OK!
```

4. Type the following command to delete the existing default route:

```
route delete 0.0.0.0 mask 0.0.0.0 192.168.0.1
```



```
C:\Users\Administrator>route delete 0.0.0.0 mask 0.0.0.0 192.168.0.1
 OK!
```

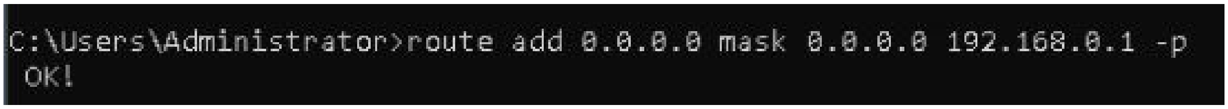
- The first octet shows the destination network, and 0.0.0.0 shows the default route.
- The second octet shows the destination network's subnet mask.
- The third octet shows the IP address of the interface on the router.

5. When you go back and look at the route help screen, you will see the entry for the **–p** option, which will make the route persistent.

   "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."

   To add a persistent default route that points to the IP address of the default gateway, type the following command:

```
route add 0.0.0.0 mask 0.0.0.0 192.168.0.1 -p
```

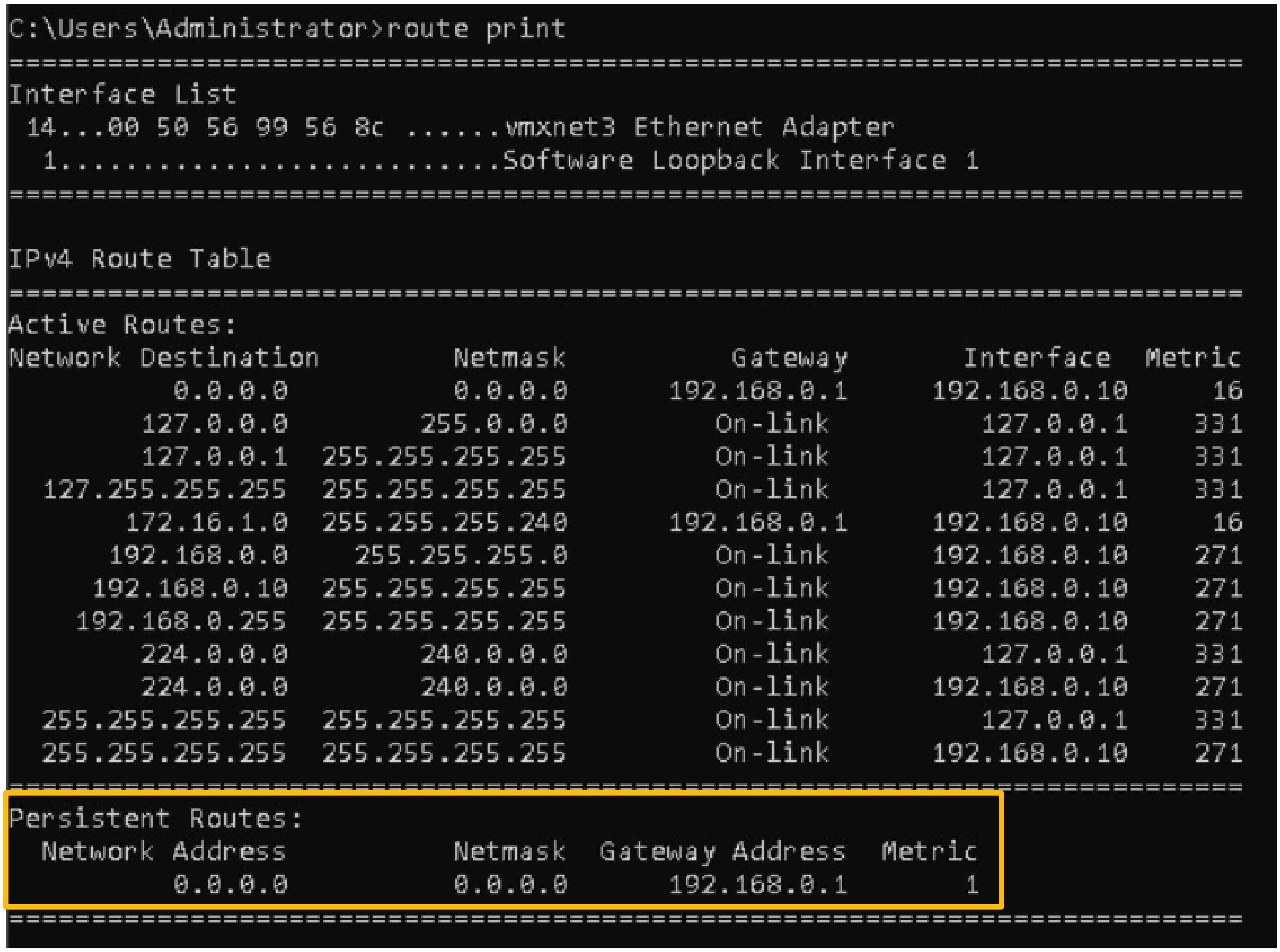


```
C:\Users\Administrator>route add 0.0.0.0 mask 0.0.0.0 192.168.0.1 -p
 OK!
```

6. Display the routing table again by typing:

```
route print
```

The default route is now listed as persistent.



```
C:\Users\Administrator>route print
===========================================================================
Interface List
 14...00 50 56 99 56 8c ......vmxnet3 Ethernet Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.10     16
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
       172.16.1.0  255.255.255.240      192.168.0.1    192.168.0.10     16
      192.168.0.0    255.255.255.0         On-link      192.168.0.10    271
     192.168.0.10  255.255.255.255         On-link      192.168.0.10    271
    192.168.0.255  255.255.255.255         On-link      192.168.0.10    271
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.0.10    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.0.10    271
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.0.1       1
===========================================================================
```

4. Leave the *WinOS* machine open and continue to the next task.

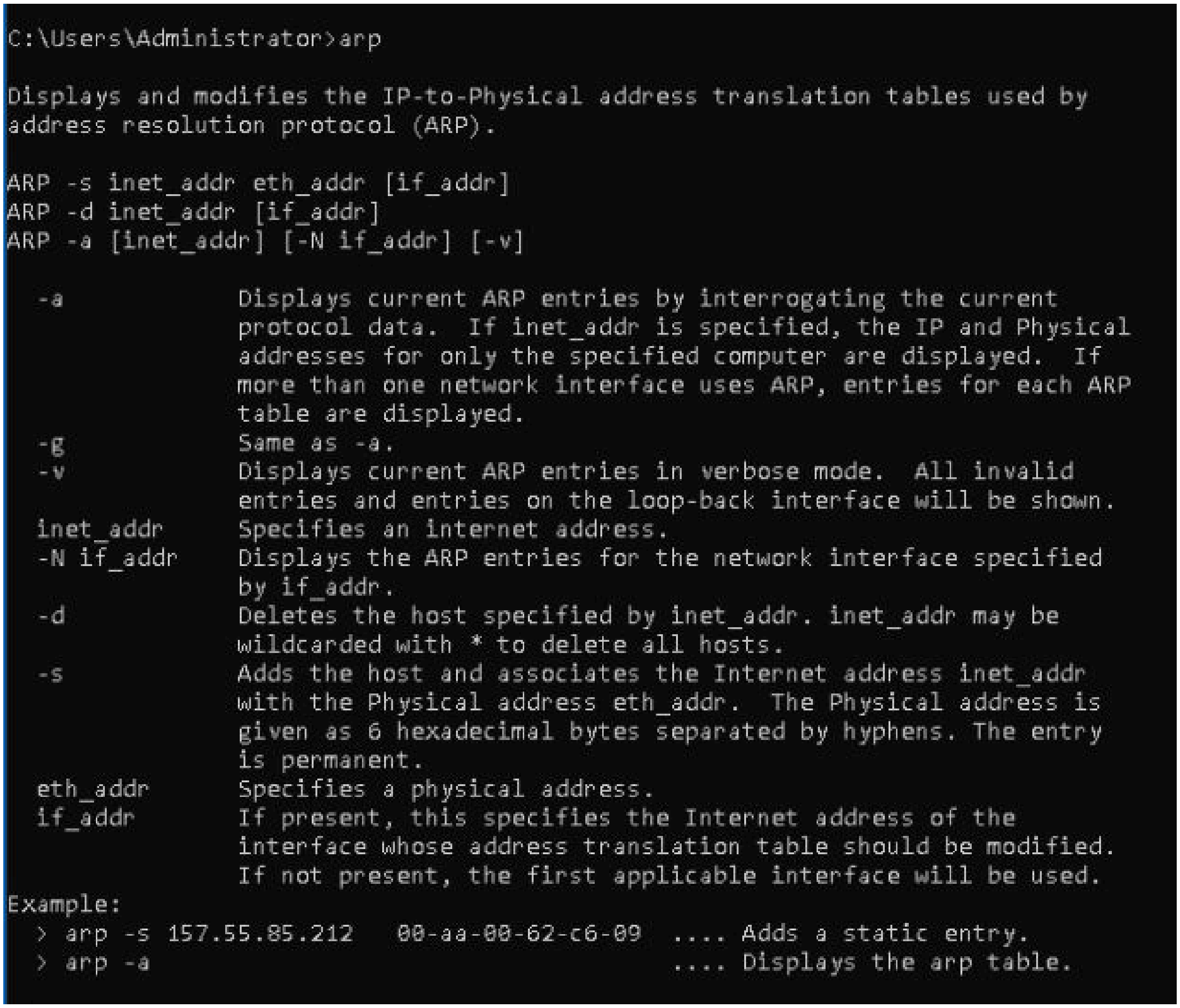
5 Using ARP

ARP (Address Resolution Protocol) is the protocol that is used to bridge between OSI Layer 2 protocols, such as Ethernet and WIFI, and OSI Layer 3 protocols, primarily IP. It is used to map Layer 2 MAC addresses with their corresponding IP addresses. The tables are kept in the memory of the hosts that reside on a local network. The table is built dynamically as hosts are contacted (such as by a *ping*).

The *ARP* protocol is used for host-to-host connectivity and rarely requires human intervention. But, it is important to monitor the status of the ARP tables because they can be compromised by hackers and become a vector for malware.

1. In the command prompt window, type the following command to show the *ARP* help screen.

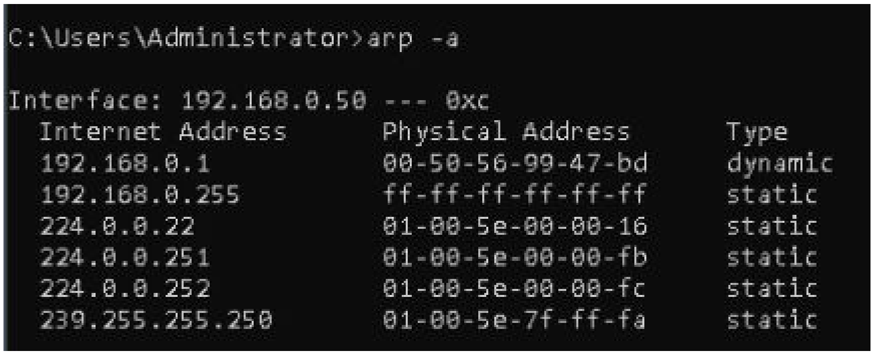
```
arp
```



```
C:\Users\Administrator>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -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.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  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. inet_addr may be
                wildcarded with * to delete all hosts.
  -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.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

2. To display the *ARP* table for all the interfaces on the host, type the following command:

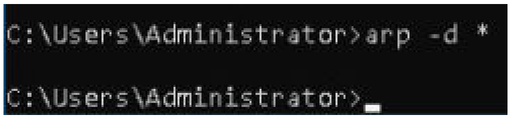
```
arp -a
```



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

Interface: 192.168.0.50 --- 0xc
  Internet Address      Physical Address      Type
  192.168.0.1           00-50-56-99-47-bd     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     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
```

3. To clear all of the dynamic entries in the *ARP* table, type the following command:

```
arp -d *
```

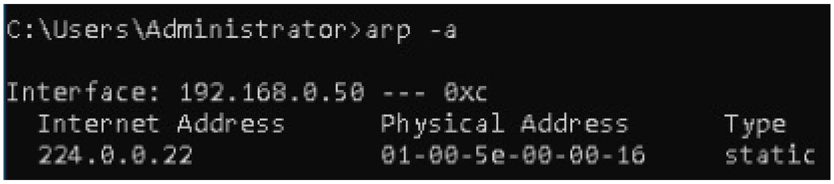


```
C:\Users\Administrator>arp -d *

C:\Users\Administrator>_
```

If the command executed correctly, you will not get any reply message.

4. To confirm the table has been cleared of all dynamic *ARP* entries, type the command:

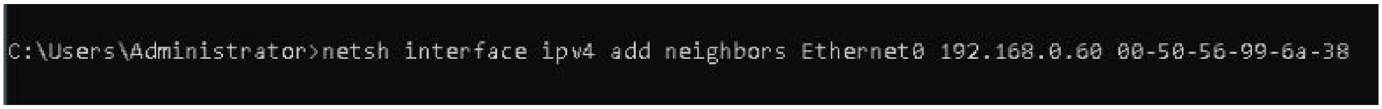
```
arp -a
```



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

Interface: 192.168.0.50 --- 0xc
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
```

5. To add a static *ARP* entry to the *MintOS* computer (*192.168.0.60*), type the following command:

```
netsh interface ipv4 add neighbors Ethernet0 192.168.0.60 00-50-56-99-6a-38
```

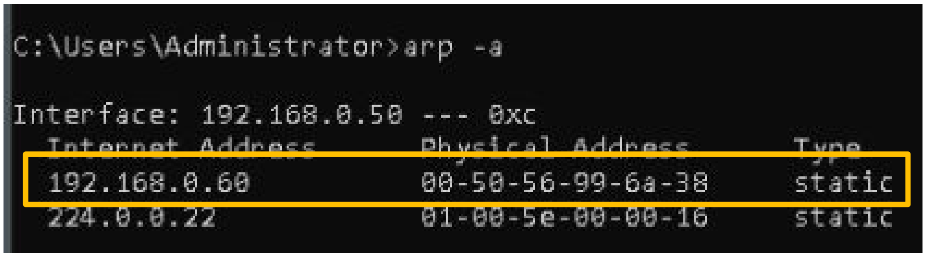


```
C:\Users\Administrator>netsh interface ipv4 add neighbors Ethernet0 192.168.0.60 00-50-56-99-6a-38
```

6. Display the *ARP* table to show the new entry by typing the following command:

```
arp -a
```

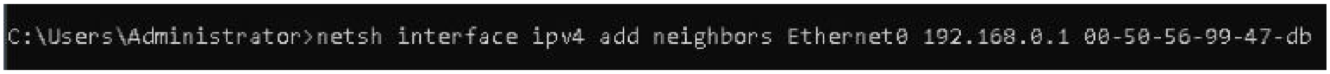
Notice that the IP address is now a static entry in the *ARP* table.



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

Interface: 192.168.0.50 --- 0xc
  Internet Address      Physical Address      Type
  192.168.0.60          00-50-56-99-6a-38     static
  224.0.0.22            01-00-5e-00-00-16     static
```

7. It's a good idea to add a static *ARP* table entry for the default gateway. Type the following command:

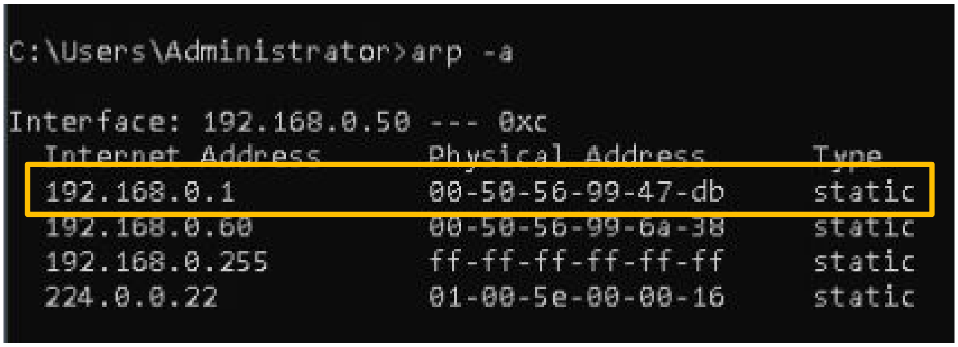
```
netsh interface ipv4 add neighbors Ethernet0 192.168.0.1 00-50-56-99-47-db
```



```
C:\Users\Administrator>netsh interface ipv4 add neighbors Ethernet0 192.168.0.1 00-50-56-99-47-db
```

8. Display the *ARP* table to show the default gateway entry by typing the following command:

```
arp -a
```



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

Interface: 192.168.0.50 --- 0xc
  Internet Address      Physical Address      Type
  192.168.0.1           00-50-56-99-47-db     static
  192.168.0.60          00-50-56-99-6a-38     static
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
```

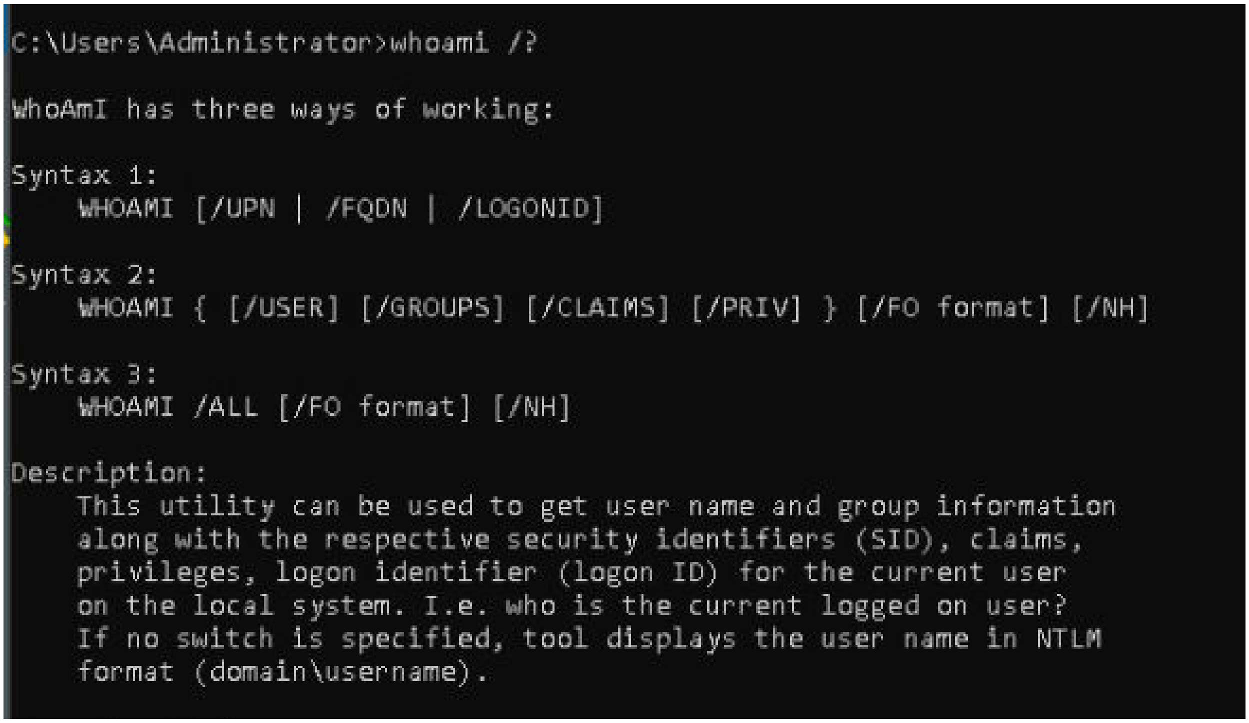
9. Leave the *WinOS* machine open and continue to the next task.

6 Using WHOAMI

The *whoami* command is used to identify the current user on the system, display a list of users in the local database, identify their permissions/roles, and check the login history.

1. In the command prompt window, type the following command to show the *whoami* help screen.

```
whoami /?
```

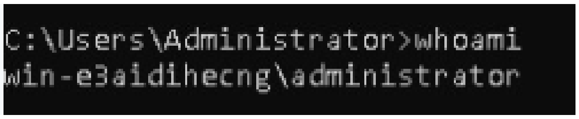


```
C:\Users\Administrator>whoami /?

WhoAmI has three ways of working:

Syntax 1:
    WHOAMI [/UPN | /FQDN | /LOGONID]

Syntax 2:
    WHOAMI { [/USER] [/GROUPS] [/CLAIMS] [/PRIV] } [/FO format] [/NH]

Syntax 3:
    WHOAMI /ALL [/FO format] [/NH]

Description:
    This utility can be used to get user name and group information
    along with the respective security identifiers (SID), claims,
    privileges, logon identifier (logon ID) for the current user
    on the local system. I.e. who is the current logged on user?
    If no switch is specified, tool displays the user name in NTLM
    format (domain\username).
```

2. The basic *whoami* command will display the **Domain Name** and the currently logged-in **User Name**. In **Windows**, a **Domain** is a network of computers, printers, user accounts, and other resources that are registered to a distributed database residing on one or more computers, called **Domain Controllers**. In **Windows**, the domain and the database are managed by a system called **Active Directory**.

   To display the **Domain Name** and **User Name**, type the following command:

```
whoami
```

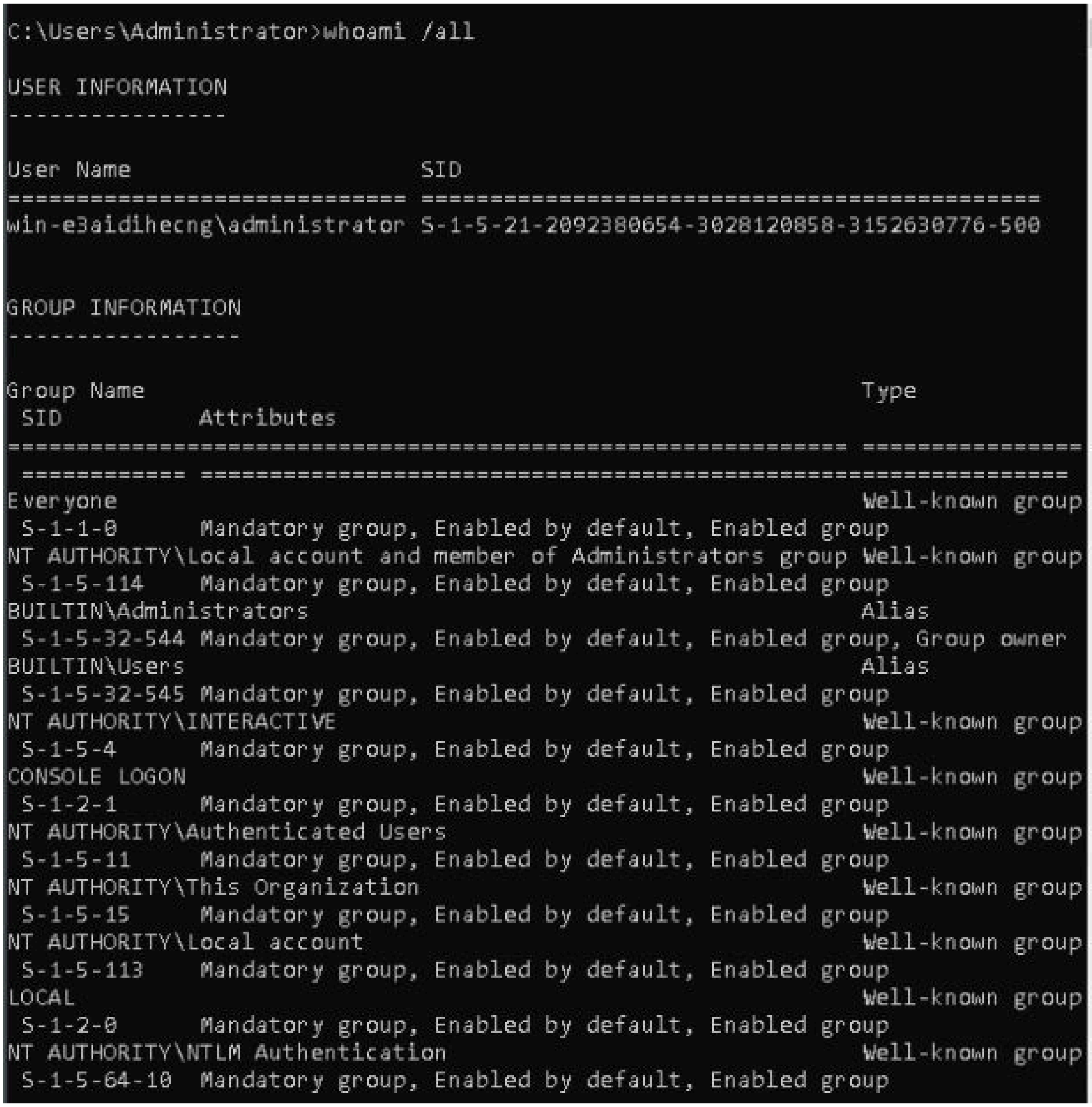


```
C:\Users\Administrator>whoami
win-e3aidihecng\administrator
```

If the computer is not registered to a Domain, the computer name will be displayed.

3. To display all of the information that is in the current access token, including the current user name, security identifiers (SID), privileges, and groups that the current user belongs to, type the following command:

```
whoami /all
```



```
C:\Users\Administrator>whoami /all

USER INFORMATION
----------------

User Name                     SID
============================= ==============================================
win-e3aidihecng\administrator S-1-5-21-2092380654-3028120858-3152630776-500


GROUP INFORMATION
-----------------

Group Name                                                     Type
 SID          Attributes
============================================================= ================
 ============ ===============================================================
Everyone                                                      Well-known group
 S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group
 S-1-5-114    Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                        Alias
 S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                                                 Alias
 S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group
 S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                                 Well-known group
 S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group
 S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                                Well-known group
 S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                    Well-known group
 S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                                         Well-known group
 S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group
 S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
```

An access token is an object that describes the security context, which are the attributes or rules associated with the user object.

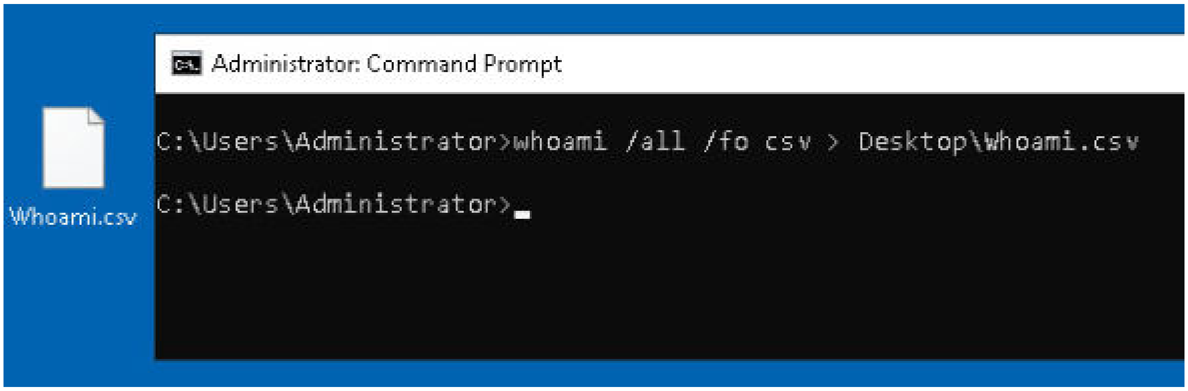
"When a user logs on, the system verifies the user's password by comparing it with information stored in a security database. If the password is authenticated, the system produces an access token. Every process executed on behalf of this user has a copy of this access token."

https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens

4. To send the output to a **CSV** (comma-separated values) file, type the following command:

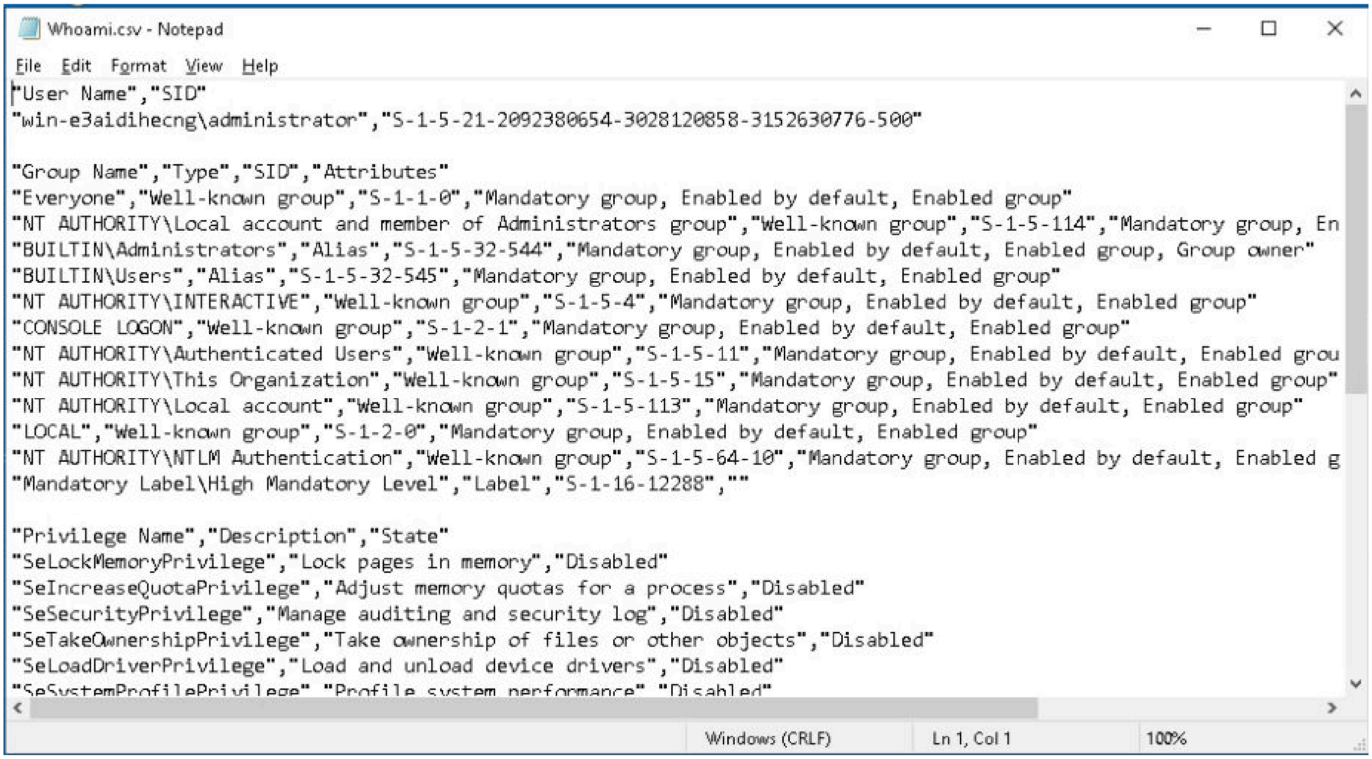
```
whoami /all /fo csv > Desktop\Whoami.csv
```

In the command, the **/fo csv** means to format output as a **CSV**.
The **>** will direct the output to the file **Desktop/Whoami.csv**



```
C:\Users\Administrator>whoami /all /fo csv > Desktop\Whoami.csv

C:\Users\Administrator>_
```

The **CSV** file can be used for documentation.



```
"User Name","SID"
"win-e3aidihecng\administrator","S-1-5-21-2092380654-3028120858-3152630776-500"

"Group Name","Type","SID","Attributes"
"Everyone","Well-known group","S-1-1-0","Mandatory group, Enabled by default, Enabled group"
"NT AUTHORITY\Local account and member of Administrators group","Well-known group","S-1-5-114","Mandatory group, En
"BUILTIN\Administrators","Alias","S-1-5-32-544","Mandatory group, Enabled by default, Enabled group, Group owner"
"BUILTIN\Users","Alias","S-1-5-32-545","Mandatory group, Enabled by default, Enabled group"
"NT AUTHORITY\INTERACTIVE","Well-known group","S-1-5-4","Mandatory group, Enabled by default, Enabled group"
"CONSOLE LOGON","Well-known group","S-1-2-1","Mandatory group, Enabled by default, Enabled group"
"NT AUTHORITY\Authenticated Users","Well-known group","S-1-5-11","Mandatory group, Enabled by default, Enabled grou
"NT AUTHORITY\This Organization","Well-known group","S-1-5-15","Mandatory group, Enabled by default, Enabled group"
"NT AUTHORITY\Local account","Well-known group","S-1-5-113","Mandatory group, Enabled by default, Enabled group"
"LOCAL","Well-known group","S-1-2-0","Mandatory group, Enabled by default, Enabled group"
"NT AUTHORITY\NTLM Authentication","Well-known group","S-1-5-64-10","Mandatory group, Enabled by default, Enabled g
"Mandatory Label\High Mandatory Level","Label","S-1-16-12288",""

"Privilege Name","Description","State"
"SeLockMemoryPrivilege","Lock pages in memory","Disabled"
"SeIncreaseQuotaPrivilege","Adjust memory quotas for a process","Disabled"
"SeSecurityPrivilege","Manage auditing and security log","Disabled"
"SeTakeOwnershipPrivilege","Take ownership of files or other objects","Disabled"
"SeLoadDriverPrivilege","Load and unload device drivers","Disabled"
"SeSystemProfilePrivilege","Profile system performance","Disabled"
```

5. The lab is now complete; you may now end the reservation.