|  |  |  |
| --- | --- | --- |
| Agpoon, Claire | Information Assurance & Security 1 |  |
| BSIT 3A  List of common TCP/IP Protocols: | Mr. Gabriel Thomas Torneros | 2-22-24 |

|  |  |  |
| --- | --- | --- |
| **TCP/IP** | **USES/ DESCRIPTION** | **PORTS** |
| File Transfer Protocol (FTP) | It is one most commonly used on the internet and  within Private networks. | 20 & 21 |
| Secure Shell | It is the primary method used to manage a network device.  Typically used as secure alternative to Telnet which does not support secure  connections. | 22 |
| Telnet | It is primary method used to manage network devices at the command level. Unlike to SSH it does not simply provides a basic unsecured connection. | 23 |
| Simple Mail Transfer Protocol (SMTP) | It is used for two primary functions. Used to transfer mail(email) from source to destination, 2nd used by end users to send email to mail  system. | 25 |
| Domain Name System (DNS) | It is used widely on public internet and on private networks to translate domain  names into IP Address. | 53 |
| Dynamic Host Configuration Protocol (DHCP) | It is used on networks that can’t use static IP Address. | 67 & 68 |
| Trivial File Transfer Protocol (TFTP) | Method of file transfer without the session  requirements that FTP uses. | 69 |
| Hyper Text Transfer Protocol (HTTP) | It is the main protocol used by web browsers. Also one of most commonly used  protocols on networks. | 80 |
| Post Office Protocol (POP) v3 | Version 3 is one of 2 main protocols used to retrieve  mail from a server. | 110 |
| Network Time Protocol (NTP) | It is used to synchronize the  devices on the internet. | 123 |
| NetBIOS | Is not a protocol but its  typically used in combination | 137 & 138 & 139 |

|  |  |  |
| --- | --- | --- |
|  | with IP with the NetBIOS over  TCP/IP (NBT) Protocol. |  |
| Internet Message Access Protocol (IMAP) | Version 3 is the 2nd main protocols used to retrieve  mail from a server. | 143 |
| Simple Network Management Protocol  (SNMP) | Its used by Network Administrators as a method  of network management. | 161 &162 |
| Border Gateway Protocol (BGP) | Version 4 widely used on the public internet and by Internet Service Providers to maintain a large routing  tables and traffic processing. | 179 |
| Lightweight Directory Access Protocol (LDAP) | It provides mechanism of accessing and maintaining distributed directory  information. | 389 |
| Hyper Text Transfer Protocol  Over SSL/TLS (HTTPS) | Used in conjunction with http  to provide the same services. | 443 |
| Lightweight Directory Access Protocol over TLS/SSL (LDAPS) | Just like https, it provides same function as LDAP but over a secure connection,  which provided by SSL/TSL. | 639 |
| FTP over TLS/SSL | Just like the two entries above, it uses the FTP protocol which is then  secured using SSL/ TLS. | 989 & 990 |
| Message Send Protocol (MSP) | Used to send short message between nodes and network.  A short message is transmitted from the sender to the receiver over the  connection. | 18 |
| Discard Protocol (DP) | It designed for testing,  debugging, measurement and host management. | 9 |
| TCP Port Service Multiplexer (TCPMUX) | Enables servers to provide multiple services without needing dedicated ports for  each service. | 1 |
| Day Time Protocol (DTP) | It is a simple protocol used to retrieve a current time from  remote server. | 37 |
| Character Generation Protocol (CHARGEN) | Its for testing, debugging and measurement purposes. This  protocol is rarely use. | 19 |
| Kerberos | It is network authentication  protocol provides strong | 88 |

|  |  |  |
| --- | --- | --- |
|  | authentication for client/ server apps by using secret  key cryptography. |  |

List of all error messages:

# 100 Status Codes – informational responses

100: Continue -This code means the server in question has received your browser’s request headers and is now ready for the request body to be sent.

101: Switching Protocols - Your browser has asked the server to change protocols and the server has agreed.

103: Early Hints - This returns some response headers before the final http message.

# 200 Status Codes – success responses

200: Ok - The standard response for successful http requests. 201: Created - The request has been fulfilled.

202: Accepted - The request has been accepted for processing, but the processing has not been completed. The request may or may not be acted upon and may be disallowed when the processing does occur.

203: Non-authoritative information -This code appears when a proxy is in use and means the proxy server received http code 200, everything is okay, from the origin server, but has modified the response before passing it on to your browser session.

204: No content - This code means the server has successfully processed the request, but it’s not going to return any content.

205: Reset content - This is similar to the 204 code in that the server has successfully processed the request, but it’s not going to return any content and the document view will be reset.

206: Partial content - You may see this status code if your http client uses range headers. This enables the browser to perform tasks like resuming paused downloads and splitting downloads into multiple streams. This code is sent when a range header causes the server to send only part of the requested resource.

# 300 Status Codes – Redirection Responses

300: Multiple Choices - Sometimes there may be multiple processing resources the server can respond with to fulfill the browser’s request. A 300 code means your browser needs to choose between them. This may occur if there are multiple file type extensions available or if the server is experiencing word-sense disambiguation.

301: The requested resource has been moved permanently - This code is delivered when a web page or resource has been permanently replaced with a different one. It’s used for permanently redirecting a URL from one place to another.

302: The requested resource has moved, but was found - This code indicates the resource the browser is requesting was found, but not at the location the browser expected it. It’s used for temporarily redirecting a URL from one place to another.

303: See Other - This code tells your browser that it found the resource you requested via one of the HTTP Request Methods, such as POST, PUT, or DELETE, but to retrieve it using the other method GET you have to issue that request to a different URL than the one you originally used.

304: The requested resource has not been modified since the last time you accessed it - This code tells your browser if it has a copy of the page already in the cache, it’s okay to use it because the content on it didn’t change since it was last cached.

307: Temporary Redirect - This code has replaced 302 “Found” as the appropriate action when a resource has been temporarily moved to a different or new URL.

308: Permanent Redirect - This code is the successor to the 301 code.

# 400 Status Codes – Client Error Responses

400: Bad Request - This code means the server can’t return any response due to an error at the client’s end.

401: Unauthorized -This code is returned by the server when the resource you’re trying to access is requested without the proper authorization credentials. If you’ve set htpassword authentication, you’ll see this if you don’t login properly.

402: Payment Required - This is a somewhat obscure error and was originally intended for use in a different industry. However, that never happened, so instead the code is used by a few platforms to indicate that a request cannot be fulfilled.

The Google Developer API will give this error when you have reached the daily request limit. Shopify will give you this error if you haven’t paid your store fees and the store is temporarily suspended/deactivated.

Stripe will show you this error if your payment failed or they are blocking a transaction. 403: Access to that resource is forbidden - This code is returned when a user attempts to access something they don’t have permission to view. If you’re trying to access password- protected content without first logging in, you would probably see this error.

404: The requested resource was not found - This means the URL / content the browser requested isn’t on the server.

405: Method not allowed - This is generated when the web server supports the method received, but the target resource doesn’t.

406: Not acceptable response - The resource requested is capable of generating only content that is not acceptable according to the accepted headers sent with the request.

407: Proxy Authentication Required - A proxy server is in use and requires your browser to authenticate itself to continue.

408: The server timed out waiting for the rest of the request from the browser - This code is generated when the server times out while waiting for the full request from the browser.

409: Conflict - A 409 status code means the server couldn’t process the request from the browser because there’s a conflict with the relevant resource. This typically happens when there are multiple edits happening to the page simultaneously.

410: The requested resource is gone and won’t be coming pack - This is similar to a 404, but indicates to the browser this was expected, rather than unexpected, and is also very permanent. 411: Length Required - This means the requested resource requires the client to specify a

certain length, and the client didn’t.

412: Precondition failed - Your browser included certain conditions in the request headers and the server didn’t meet those specs.

413: Payload too large - Or Request Entity Too Large. Your request is larger than the server is willing/able to process.

414: URI Too Long - This means a GET request has been encoded as a query string that is too large for the server to process.

415: Unsupported Media Type - This means your request was for a media type the server or resource doesn’t support.

416: Range Not Satisfiable - Your request was for a portion of a resource the server isn’t able to return.

417: Expectation failed - The server is unable to meet the requirements stated in the requests expect header field.

418: I’m a teapot - This is returned by teapots that receive requests to brew coffee. It’s an April Fools Joke.

422: Processable Entity - The client request contains semantic errors and the server can’t process it.

425: Too Early - This error is sent when the server is unwilling to process a request because it may be replayed.

426: Upgrade required - Due to the contents of the requests upgrade header field, the client needs to switch to a different protocol.

428: Precondition Required - The server requires conditions to be specified before processing the request.

429: Too many requests - This is generated by the server when the user has sent too many requests in a given amount of time. Also known as rate-limiting.

431: Request Header Fields Too Large - The server can’t process the request because the header fields are too large. This may indicate a problem with a single header field or all of them. 451: Unavailable for Legal Reasons - The operator of the server has received a demand to prohibit access to the resources you have requested. Also, a reference to the famous Ray Bradbury novel Fahrenheit 451.

499: Client closed request - This code is returned by NGINX when the client closes the request while Nginx is still processing it.

# 500 Status Codes – Server Error Responses

500: There was an error on the server and the request could not be generated -This is a generic code that simply means, internal server error. Something went wrong on the server and what you’re requesting isn’t available.

501: Not implemented -This error indicates that the server does not support the functionality required to fulfill the request.

502: Bad gateway - This error code typically means that one server has received an invalid response from another, such as when a proxy server is in use.

503: The server is unavailable to handle this request right now -This code happens when a server may be overloaded and is unable to handle additional requests.

504: The server, acting as a gateway, timed out while waiting for another server to respond - This is the error returned when there are two servers involved in processing a request, and the first server times out waiting for the second one to respond.

505: HTTP Version not supported - The server doesn’t support the version of HTTP the client used to make the request.

511: Network Authentication Required - This error code is sent when the network you’re trying to use requires some form of authentication before sending your request to the server. For instance, you may need to agree to the terms and conditions of a public hotspot.

521: Web server is down -This is a Cloudflare-specific error message and means your browser was able to successfully connect to Cloudflare’s network, but it wasn’t able to connect to the origin server.

525: SSL Handshake failed - This error means that the SSL Handshake between a domain using Cloudflare and the origin web server failed.

Definition and Example of each following:

* IPConfig or Internet Protocol CONFIGuration – Is a command line utility, used to display and manage the IP address assigned to the machine or system. It is a console program application of computer operating system that display all current TCP/IP network.

Example:

Show detailed information C:\> ipconfig /all

Release and Renew all adapters:

ipconfig /release ipconfig /renew

Release and Renew all adapters - one liner for remote use:

ipconfig /release && ipconfig /renew

Renew any connection that has a name starting with EL:

ipconfig /renew EL\*

Release all connections matching \*Con\*, eg. "Local Area Connection 1" or "Local Area Connection 2":

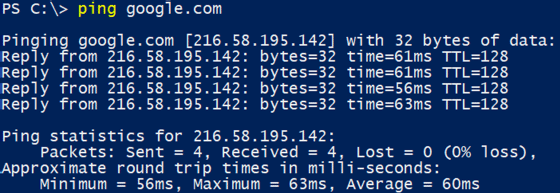
ipconfig /release \*Con\*

Set the DHCP class ID for the named adapter to TEST:

ipconfig /setclassid "Local Area Connection" TEST

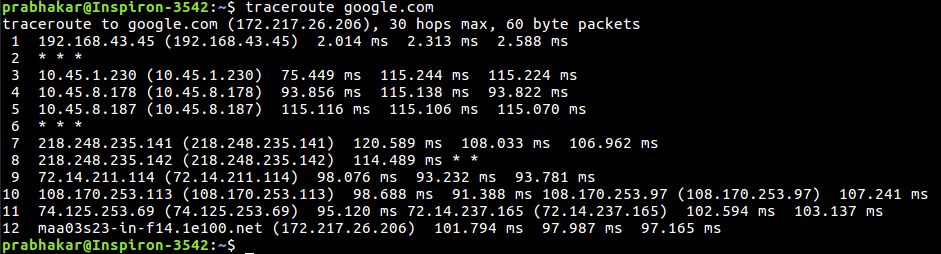
* Ping or (Packet Internet or Inter-Network Groper) – It is a basic program that allow a user to test and verify a particular destination of IP address. It is also used diagnostically ensure that a host computer, user is trying to reach is operating.

Example: users can go to the command prompt screen (start/run/cmd) and enter ping xxxxx.yyy, where xxxxx is the second-level domain name, like "whatis," and yyy is the top-level domain name, like "com."



* + Tracert or (Trace Route) – It can use to trace the path that an Internet Protocol (IP) packet takes to its destination.

Example: Tracert in Linux



* + Netstat or (Network Statistics) – It can report the status of TCP/IP and Ethernet connections.

Following are some of the commands used in the Windows version of netstat.

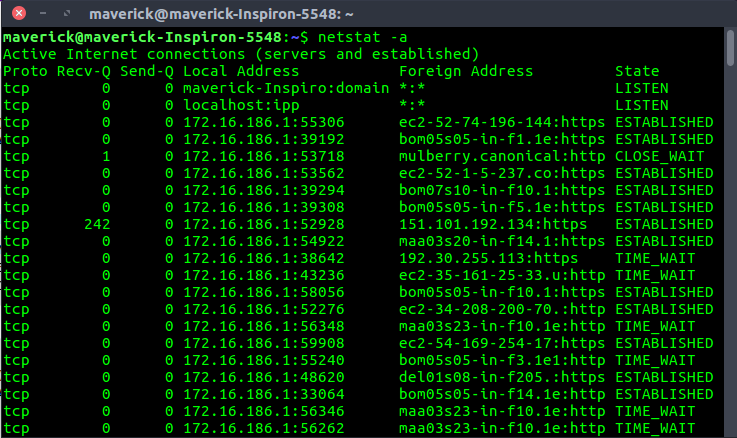
Command Purpose

netstat ? Help with commands netstat -a Active ports

netstat -e Ethernet statistics netstat -r Routing table

netstat -s Stats for all protocols netstat -sp udp Stats for UDP protocol

Example:



* + NS look up or (Name Server lookup) – It can displays the IP address of hostname or tool for querying the DNS to obtain the mapping between domain name and IP address.

Example:







