

# N00B HACK3RS COMMUNITY, (NHC)

## Daily Activity - 2

July 17, 2020



Topic : What's Network protocols & what's Dark, Deep & Surface Web???

---

## Network Protocol :

Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed. The most popular model used to establish open communication between two systems is the Open Systems Interface (OSI) model proposed by ISO. [cc] <https://tutorialspoint.com>

## Types of Standard Network Protocols :

1. HTTP : HyperText Transfer Protocol	Port	80
2. HTTPS : HyperText Transfer Protocol Secure	Port	443
3. IP : Internet Protocol		
4. DHCP : Dynamic Host Configuration Protocol		
5. SMTP : Simple Mail Transfer Protocol	Port	25
6. SNMP : Simple Network Management Protocol	Port	161
7. IMAP/IMAP4 : Internet Message Access Protocol v4		
8. POP3 : Post Office Protocol v3	Port	110
9. SSL/TLS :Secure Socket Layer/Transport Layer Security		
10. SSH/Telnet : Secure Shell/Telnet	Port	22
11. FTP : File Transfer Protocol	Port	21
12. RDP : Remote Desktop Protocol	Port	3389

---

## 1. HTTP : HyperText Transfer Protocol :

HTTP is the key protocol for being able to transfer data across the Internet. HTTP allows the transfer of HyperText Markup Language (HTML) and other related scripting languages (like CSS) to travel from servers to browsers. The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load web pages using hypertext links.

HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

**HTTP Requests :** Each http request made across internet carries with it series of encoded data that carries different type information :

1. HTTP Version Type (HTTP/0.9/1.0/1.1)
2. A Url
3. An HTTP Method (GET, POST, OPTIONS, etc)
4. HTTP Request Header
5. Optional HTTP Body

An HTTP method : HTTP verb, indicates the action that the HTTP request expects from the queried server. For example, two of the most common HTTP methods are 'GET' and 'POST';

GET : A 'GET' request expects information back in return (usually in the form of a website),

POST : while a 'POST' request typically indicates that the client is submitting information to the web server (such as form information, e.g. a submitted username and password).

OPTIONS : Tells about how many HTTP Verbs are active on a web server.



---

**HTTP Request Header** : (Google.com)


▼ **Request Headers**

**:authority:** www.google.com  
**:method:** GET  
**:path:** /  
**:scheme:** https  
**accept:** text/html  
**accept-encoding:** gzip, deflate, br  
**accept-language:** en-US,en;q=0.9  
**upgrade-insecure-requests:** 1  
**user-agent:** Mozilla/5.0

**HTTP Response Header** : is what web clients (often browsers) receive from an Internet server in answer to an HTTP request. These responses communicate valuable information based on what was asked for in the HTTP request.

1. An HTTP status code
2. HTTP response headers
3. Optional HTTP body

**HTTP Status Code** : codes are 3-digit codes most often used to indicate whether an HTTP request has been successfully completed. Status codes are broken into the following 5 blocks:

1. 1xx Informational
  2. 2xx Success
  3. 3xx Redirection
  4. 4xx Client Error
  5. 5xx Server Error
- 

---

**HTTP Response Header :** (Google.com)

▼ **Response Headers**

**cache-control:** private, max-age=0  
**content-encoding:** br  
**content-type:** text/html; charset=UTF-8  
**date:** Thu, 21 Dec 2017 18:25:08 GMT  
**status:** 200  
**strict-transport-security:** max-age=86400  
**x-frame-options:** SAMEORIGIN

**HTTP Responses Body :** Generally response body contains html,css and js code.

For more Overview on HTTP Visit : [Security Testing - HTTP Protocol Basics](#)

[HTTP --> w3.org](#)

## 2. HTTPS : HyperText Transfer Protocol Secure

HTTPS and a secure version of HTTP. The Hypertext Transfer Protocol Secure (HTTPS) protocol facilitates secure communication over a network. Strictly speaking, HTTPS is a layer on top of HTTP using SSL.

## 3. IP : Internet Protocol

The Internet Protocol is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet

Port : The port of an IP address is always associated with it.



---

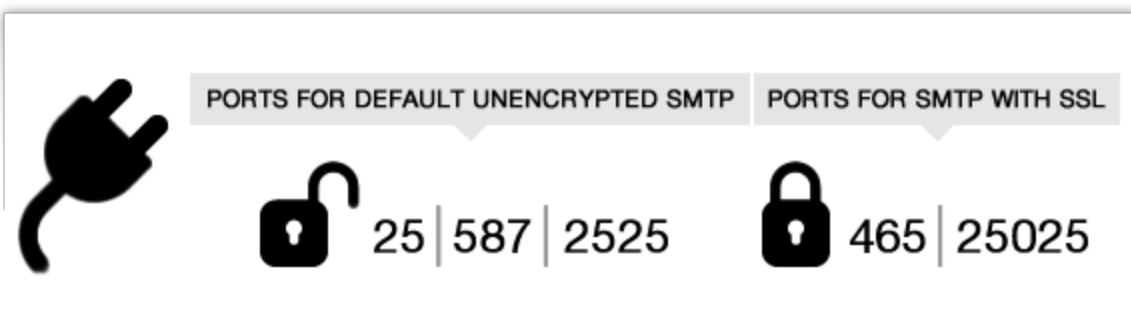
## 4. DHCP : Dynamic Host Configuration Protocol

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters. Requests for comments (RFC) 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF)- defined standard based on the BOOTP protocol.

## 5. SMTP : Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol is the protocol for Internet email. It transfers email amongst computers. The majority of computers in the wild understand SMTP, but some do not.

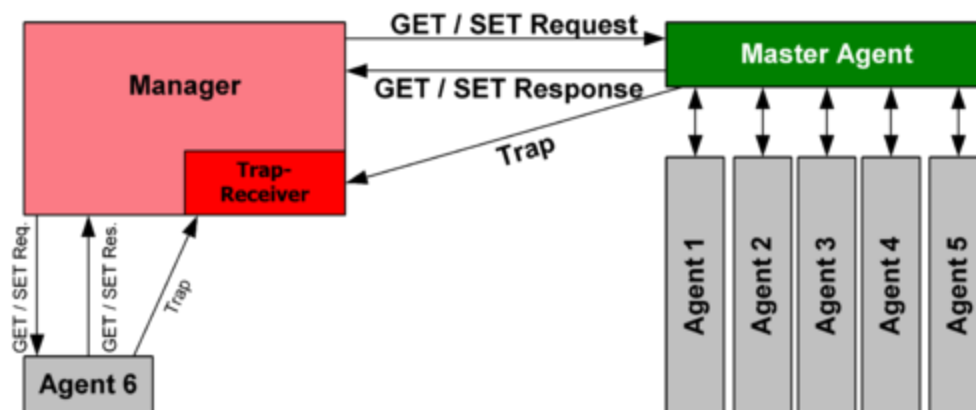


---

## 6. SNMP : Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response is sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162.



## 7. IMAP4 : Internet Message Access Protocol Version 4

The Internet Message Access Protocol and POP3 are sort of connected. Abbreviated to IMAP, this protocol provides a richer set of features when compared to POP3. Worth mentioning that although IMAP and POP3 both help to manage email, they cannot function together, i.e. the user must choose one or the other.



IMAP4 includes a number of features that are not supported by POP3. Specifically, IMAP4 allows users to :

1. Access multiple folders, including public folders
2. Create hierarchies of folders for storing messages
3. Leave messages on the server after reading them so that they can access the messages again from another location
4. Search a mailbox for a specific message to download
5. Flag messages as read
6. Selectively download portions of messages or attachments only
7. Review the headers of messages before downloading them

To retrieve a message from an IMAP4 server, an IMAP4 client first establishes a Transmission Control Protocol (TCP) session using TCP port 143. The client then identifies itself to the server and issues a series of IMAP4 commands:

1. LIST: Retrieves a list of folders in the client's mailbox
2. SELECT: Selects a particular folder to access its messages
3. FETCH: Retrieves individual messages
4. LOGOUT: Ends the IMAP4 session



---

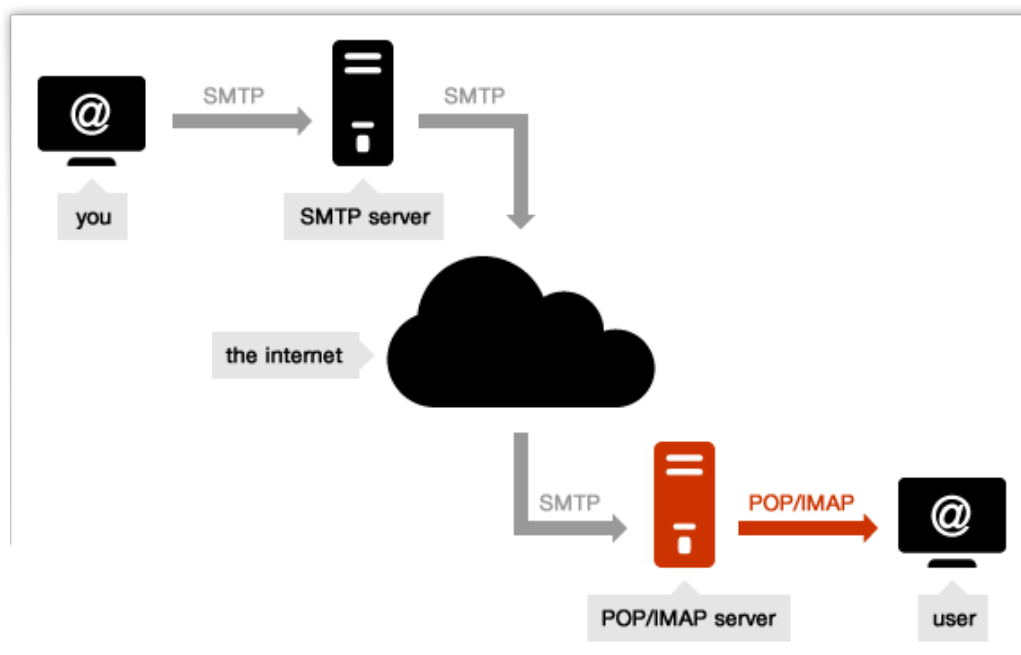
## 8. POP3 : Post Office Protocol Version 3

The Post Office Protocol (latest version is '3') provides basic client/ server features that help the user download email from a POP3 email server to a computer (be it mobile or a desktop). The main purpose of the protocol is to allow users to access their email more freely.

Post Office Protocol (POP) is a type of computer networking and Internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine.

POP is an application layer protocol in the OSI model that provides end users the ability to fetch and receive email.

**Port :** By default, the POP3 protocol works on two ports: Port 110 - this is the default POP3 unencrypted port. Port 995 - this is the port you need to use if you want to connect using POP3 securely.



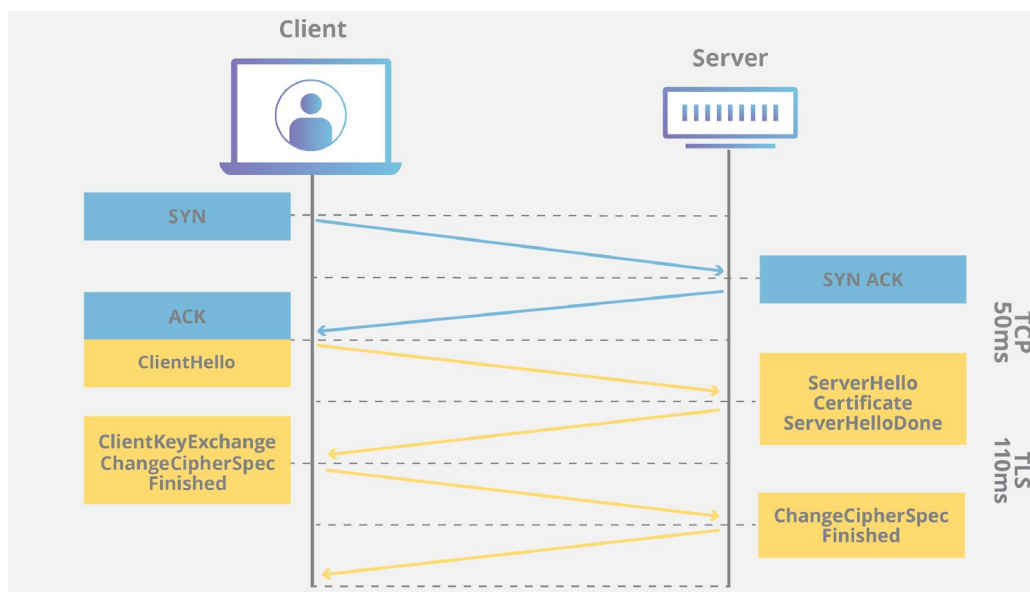
## 9. SSL/TLS : Secure Socket Layer/Transport Layer Security

SSL/TLS both are encryption protocols used to encrypt the data over the internet. TLS evolved from a previous encryption protocol called Secure Socket Layer (SSL), which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

### How does TLS works :

TLS can be used on top of a transport-layer security protocol like TCP. There are three main components to TLS: Encryption, Authentication, and Integrity.

1. **Encryption:** hides the data being transferred from third parties.
2. **Authentication:** ensures that the parties exchanging information are who they claim to be.
3. **Integrity:** verifies that the data has not been forged or tampered with.



---

A TLS connection is initiated using a sequence known as the TLS handshake. The TLS handshake establishes a cypher suite for each communication session. The cypher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session. TLS is able to set the matching session keys over an unencrypted channel thanks to a technology known as public key cryptography.

### Implementation of TLS/SSL in a Website :

All Cloudflare users automatically have HTTPS protection from Cloudflare. Via Universal SSL, Cloudflare offers free TLS/SSL certificates to all users. Anyone who doesn't use Cloudflare will have to acquire an SSL certificate from a certificate authority, often for a fee, and install the certificate on their origin servers.

## 10. SSH/Telnet : Secure Shell & Telnet

SSH is a network protocol used to remotely access and manage a device. The key difference between Telnet and SSH is that SSH uses encryption, which means that all data transmitted over a network is secure from eavesdropping. SSH uses the public key encryption for such purposes.

**Telnet** : a user accessing a remote device must have an SSH client installed. On a remote device, an SSH server must be installed and running. SSH uses the TCP port 22 by default.

For Unix and Linux operating systems, the **OpenSSH** implementation comes free with the operating system and can be used to replace Telnet.

Command : `$ openssl s_client --connect <hostname>:443`

Command : `$ ssh -p <target> 22`

---

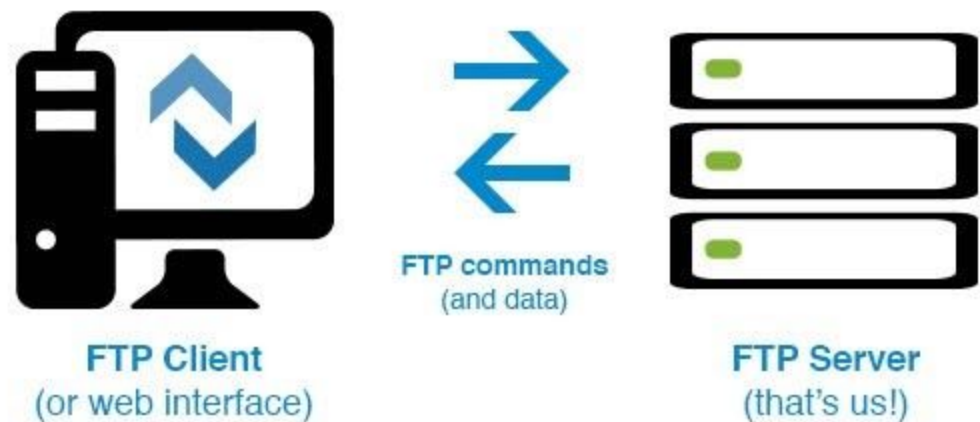
## 11. FTP : File Transfer Protocol

FTP can be defined as a standard network protocol that is especially used to transfer files from one host (machine/ operating system) to another host over a TCP/ IP based network.

To secure FTP the user can connect anonymously but only if the receiving server is configured to allow it. A better and more robust solution is to use FTPS or better still, the SSH File Transfer Protocol.

Using FTP to transfer files is helpful in these ways –

1. Easily transfers files between two different networks.
2. Can resume file transfer sessions even if connection is dropped, if protocol is configured appropriately.
3. Enables collaboration between geographically separated teams.

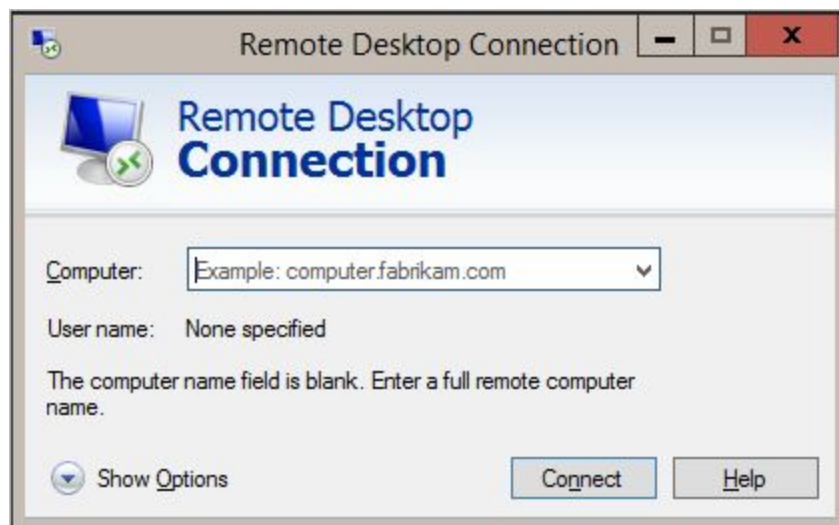


---

## 12. RDP : Remote Desktop Protocol

Remote Desktop Protocol is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

RDP allows network administrators to remotely diagnose and resolve problems that individual users encounter. To use RDP, network administrators would use RDP client software, and the individual users would use RDP server software.



RDP Server Runs on : 3389 Port

Microsoft currently refers to their official RDP client software as Remote Desktop Connection, formerly "Terminal Services Client".

---

# Read this PDF, This Is Your Assignment

**N00B HACK3RS COMMUNITY, NHC**

**Founder : Sumit Oneness**

**Co-Founder : Piyush Kaushik**

© N00B HACK3RS COMMUNITY, (NHC)  
New Delhi, India.

---

