U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

Useful Protocols

October 2023

cyberforcecompetition@anl.gov

Useful Protocols

Pre-Requisites

- **Intro to Networking**

Overview

Below we provide an overview of multiple useful protocols. This is not a complete list of protocols used today but serves as an introduction to some common ones.

SSH

SSH, or Secure Shell, is used to connect to a remote computer securely. SSH is secure as the client/server connection is authenticated using a digital certificate and passwords are encrypted. It's widely used by system administrators to control remote Linux servers. SSH uses port 22.

To log into a remote Linux machine using SSH, use the following command:

```
ssh username@ip-address or hostname
```

RDP

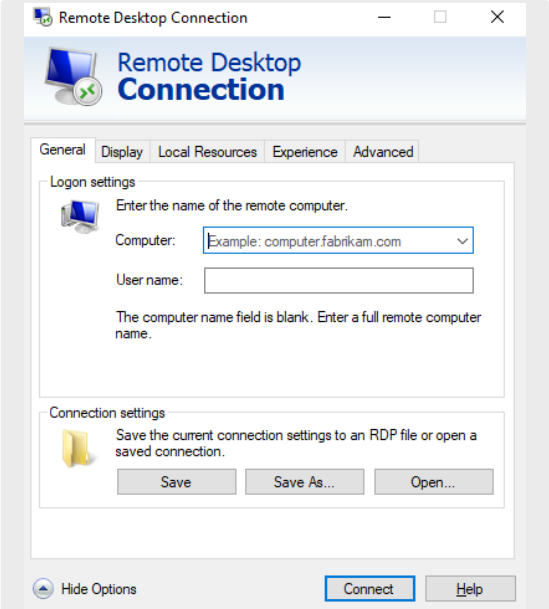
RDP, or Remote Desktop Protocol, is used for connecting to a desktop computer remotely. It is the most commonly used protocol and is available for most Windows operating systems.

Remote desktop users can access their desktop, open and edit files, and use applications like they are actually sitting at their desktop computer. Users are actually accessing their physical desktop computer and can only use files and applications that are saved locally on the desktop.

The RDP protocol opens a dedicated network channel for sending data back and forth between the connected machines, using port 3389. Mouse movements, keystrokes, the desktop display, and other data are sent over this channel using TCP/IP (the transport protocol used for most types of Internet traffic). RDP encrypts all data for security.

To set up the PC you want to connect to for remote connection, make sure to enable it in the settings. Select `Start > Settings > System > Remote Desktop` and turn on `Enable Remote Desktop`.

To use Remote Desktop to connect to the PC you just set up, search for `Remote Desktop Connection` with the search bar on the taskbar. In Remote Desktop Connection, type the hostname or the IP address of the computer you are wanting to connect to. You will also need to type the username of the account you'll use to log in.



Remote Desktop Connection Screen

If you want to launch the RDP client through PowerShell or command line use the following command: `mstsc \v:10.10.10.10:3389`.

Telnet

Telnet helps to connect to a remote Linux computer and run programs remotely and conduct administration. However, Telnet is not encrypted, as messages are sent in plaintext, so it is very insecure. Telnet uses port 23.

You can connect to it via the syntax below.

```
telnet hostname
```

You can exit by using the `logout` command.

Ping

This is used to check whether your connection to the server is healthy or not. It can also be used in analyzing network and host connections, tracking network performance and managing it, and testing hardware and software issues.

The command syntax is shown below. You can use an IP address or a website.

```
ping hostname
```

For instance, we could ping google.

```
ping google.com
```

Press Ctrl + c to exit from the ping loop.

FTP

FTP is file transfer protocol and is a preferred protocol for data transfer. You can use it to log in and establish a connection with a remote host, upload and download files, navigate through directories, and browse contents of directories. Port 21 is the default port used by the FTP server.

You can establish an FTP connection to a remote host using the command shown below.

```
ftp hostname
```

Once you enter the command, it will ask for authentication via username and password.

Then, you can use different commands to perform different actions.

Command	Function
dir	Display files in the current directory of a remote computer
cd "dirname"	Change directory to "dirname" on a remote computer
put file	Upload 'file' from local to remote computer
get file	Download 'file' from remote to local computer
quit	Logout

FTPS

FTPS, or File Transfer Protocol Secure, extends FTP by supporting Transport Layer Security (TLS) and the Secure Sockets Layer (SSL). It is a secure file transfer protocol that allows you to connect securely before sending files. Files are sent through FTPS and authenticated by FTPS supported applications, including client certificates and server identities.

FTPS supports file transfer encryption using algorithms like AES. It uses TLS to secure server connections, shielding identifiable data. It employs port identifiers for implicit and explicit connection types and uses port 990.

To connect to an FTPS server using command line, use the following command:

```
lftp -u YOUR_USER HOST_ADDRESS
```

SFTP

SFTP, or SSH File Transfer Protocol, is another secure file transfer protocol that runs over the SSH protocol. It provides the same functions as FTP and FTPS but more securely and more reliably. It protects against password sniffing and man-in-the-middle attacks. It uses encryption and cryptographic hash functions, and it authenticates both the server and user.

It uses the SSH port 22 because it is basically an SSH server. Once the user has logged in to the server using SSH, they can initiate the SFTP protocol.

To start an SFTP connection with a remote host, you can use the command:

```
sftp username@hostname
```

SFTP will then prompt you for the password to the account you're trying to log into. Then an SFTP prompt will appear like this: `sftp>`.

POP3

The Post Office Protocol (POP3) is used by local email software clients to retrieve emails from a remote mail server over a TCP/IP connection. It is a very popular protocol used by most email clients. Email servers hosted by Internet service providers also use it to receive and hold emails intended for their subscribers.

The email clients typically use the port 110 to connect to a POP3 server. However, if encrypted communication is supported on the server, users can choose to connect by using the STLS command after the protocol initiation stage or by using POP3S, which uses TLS or SSL which is on port 995.

POP3 Command	Description
`USER`	Your user name for this mail server
`PASS`	Your password
`LIST`	Message number and size of message
`DELE`	Delete selected message
`QUIT`	End the session

HTTP

The Hypertext Transfer Protocol, or HTTP, is the foundation of the Internet. It is used to load webpages using hypertext links. It is an application layer protocol designed to transfer information between networked devices. HTTP uses port 80.

An HTTP request contains the HTTP version type, a URL, an HTTP method, HTTP request headers, and an optional HTTP body.

An HTTP method indicates the action that the HTTP request expects from the queried server. Two of the most common methods are `'GET'` and `'POST'`. `'GET'` expects information back in return while `'POST'` indicates that the client is submitting information to the web server.

An HTTP request header contains text information stored in key-value pairs. They communicate core information like what browser the client is using and what data is being requested. An example is shown below.

```
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
```

The HTTP request body contains the 'body' of information the request is transferring. It has any information being submitted to the web server.

An HTTP response is what web clients receive from an Internet server in response to the HTTP request, and they communicate valuable information based on what was asked for in the request. It typically contains an HTTP status code, HTTP response headers, and an optional HTTP body.

HTTP status codes are 3-digit codes that indicate whether the 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

The 'xx' refers to different numbers between 00 and 99.

HTTP response headers convey important information like the language and format of the data being sent in the response body. An example is shown below.

```
Response Headers
        cache-control: private, max-age=0
        content-encoding: br
        content-type: text/html; charset=UTF-8
        date: Thu, 22 Jun 2023 18:25:08 GMT
        status: 200
        strict-transport-security: max-age=86400
        x-frame-options: SAMEORIGIN
```

Successful HTTP responses to `'GET'` requests typically have a body containing the requested information. Most of the time this is HTML data that a web browser will translate into a webpage.

HTTPS

Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP. HTTPS is encrypted in order to increase security of data transfer. HTTP uses port 443. Any website should use HTTPS. Web browsers nowadays mark websites that do not use HTTPS differently than those that do. Non-HTTPS websites are flagged as not secure.

HTTPS uses the TLS protocol for encryption. TLS secures communications using asymmetric public key infrastructure. This uses a private and a public key. The private key is controlled by the owner of the website and it's kept private. It lives on the web server and is used to decrypt information that's encrypted by the public key. The public key is available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted by the private key.

Information sent over HTTP is broken into packets of data that can be "sniffed" using free software so its highly vulnerable to interception. Communications that occur over HTTP occur in plain text. However, with HTTPS traffic is encrypted so that even if it is intercepted it cannot be understood.

When a user connects to a webpage, the page will send its SSL certificate which contains the public key that's needed to start the secure session. Then, the client and server go through a process called an SSL/TLS handshake, which is a series of back-and-forth communications to establish a secure connection.

DNS

The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. DNS servers allow people to input normal words into their browsers instead of every website's IP address.

A DNS server is a computer with a database containing the public IP addresses associated with the names of the websites an IP address brings a user to. Once it finds the correct IP address, browsers take the address and use it to send data to content deliver network (CDN) edge servers or origin servers. Then, the information of the website can be accessed by the user.

The URL (uniform resource locator) typed in by the user usually goes through four servers for the IP address to be provided. These servers work together to get the correct IP address to the client.

1. DNS recursor (DNS resolver): receives the query from the DNS client and communicates with other DNS servers to find the correct IP address. Once the recursor retrieves the request from the client, it acts like a client itself, making queries that get sent to the other three DNS servers.
2. Root nameservers: is designated for the internet's DNS root zone. It answers requests sent to it for records in the root zone by sending back a list of the authoritative nameservers that go with the correct TLD.
3. TLD nameservers: keep the IP address of the second-level domain contained within the TLD name before releasing the website's IP address and sending the query to the domain's nameserver.
4. Authoritative nameservers: give you the real answer to your DNS query. There are two types of authoritative nameservers: a primary nameserver (master) and a secondary nameserver (slave). The primary keeps the original copies of the zone records while the secondary is an exact copy of the primary. The secondary shares the DNS server load and acts as a backup if the primary every fails.

You can check the status of the DNS records associated with your domain and examine the nameservers to see which records are being pulled by the servers. To check on a Windows computer, you can use the `NSLOOKUP` command. First, access the Windows command prompt by either going to `Start >> command prompt` or `Run >> CMD`.

```
NSLOOKUP
set type=##
DOMAIN_NAME
```

Replace the "##" which the record type and the DOMAIN_NAME with the one you want to query. You can also find your DNS by using the command prompt and typing `ipconfig/all`.

ARP

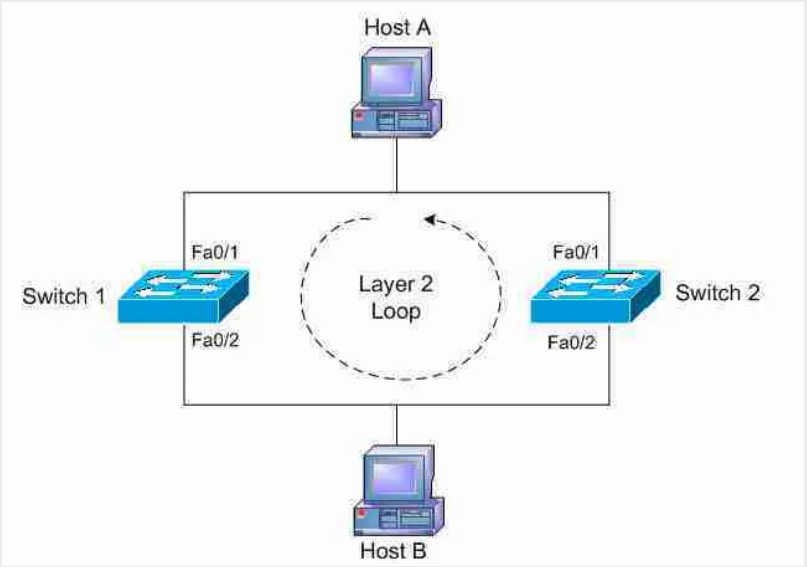
ARP, or Address Resolution Protocol, connects an IP address to a fixed physical machine address, or a MAC address, in a local-area network (LAN). This is a mapping procedure that translates these addresses, which are different lengths and would otherwise not recognize each other.

When packets of data arrive at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. ARP caches are kept on all operating systems in an IPv4 Ethernet network. Every time a device requests a MAC address to send data to another device, the device verifies its ARP cache to see if the IP-to-MAC address connection has been completed. If it hasn't, then it requests for network addresses and ARP is performed.

To display the ARP cache, you can use the `arp` command without any options. It will show the IP address, physical address, and type of ARP entries in the cache.

STP

The Spanning Tree Protocol (STP) is a loop-prevention protocol that allows switches to communicate with each other to discover physical loops in a network. If found, the STP specifies an algorithm that switches can use to create a loop-free logical topology. Loops usually occur because of multiple connections between switches, which provides redundancy.



From How to Network

More information on how STP calculates and the process can be found at source 11 below.

STP Commands	Description
`switch>enable`	Enters privileged mode

STP Commands	Description
`switch#configure terminal`	Used to enter the switch management interface
`switch(config)#spanning-tree vlan vlan-id`	Enables the spanning tree protocol on our VLAN
`switch(config)#end`	Exits configuration mode

NTP

NTP, or Network Time Protocol, synchronizes computer clock times in a network to within a few milliseconds of UTV, allowing devices connected to a TCP/IP network to work at the same adjusted time. It corrects errors in server transmission and is the foundation for time synchronization across networks.

The protocol client first requests an exchange with the time server before calculating its delay/offset and readjusting to match the server's clock. To work, there must be six-time exchanges within 10 minutes to update the clock every 10 minutes (or hourly) to maintain its time accuracy. The messages transact the updates with the User Datagram Protocol (UDP) on port 123.

To enter the mode, use the `ntp-service` command. Use the `show` command to view the current configuration, and use the `reset` command to restore default values. `cancel` exits the configuration mode without saving changes, and `exit` exits the configuration and saves changes.

IGMP

The Internet Group Management Protocol (IGMP) allows several devices to share one IP address so they can all receive the same data. It's used to set up multicasting on networks that use IPv4. Multicasting is when a group of devices all receive the same packets, which works by sharing an IP address between multiple devices. Any network traffic directed at that IP address will reach all devices that share the IP address.

IGMP uses IP addresses that are set aside for multicasting (between 224.0.0.0 and 239.255.255.255) and routers that support IGMP listen to IGMP transmissions from devices to see which devices belong to which multicast groups. When a router receives packets directed at the shared IP address, it duplicates those packets and sends copies to all members of the group. The default IGMP port is 465.

To enable IGMP on an interface use the command `set ip igmp enable`. By changing `enable` to `disable`, you can disable IGMP.

SMTP

SMTP, or Simple Mail Transfer Protocol, is used as a method to transfer mail from one user to another. It is used to send mail unlike POP3 or IMAP which is used to retrieve emails. The client who wants to send mail opens a TCP connection to the SMTP server and sends mail across it. The SMTP server is always listening and as soon as it "hears" a TCP connection from a client, it initiates a connection through port 25. After establishing connection, the client sends the mail.

The end-to-end model communicates between different organizations whereas the store-and-forward method is used within an organization. SMTP clients that want to send mail contacts the destination's host SMTP directly, and the SMTP server keeps the mail to itself until it is copied to the receiver's SMTP.

SMTP Command	Description
`HELO`	Identifies the client to the server; fully qualified domain name
`MAIL`	Initiates a message transfer; fully qualified domain of the originator
`RCPT`	Follows `MAIL` and identifies an addressee, typically with the fully qualified name; for multiple addressees, use one RCPT for each addressee
`DATA`	send data line by line

BGP

Border Gateway Protocol (BGP) is a gateway protocol that enables the internet to exchange routing information between autonomous systems. BGP makes peering possible, which allows networks to send and receive information with each other.

BGP chooses the peering option closest to where the router is. Each potential peer communicates routing information that is has and that gets stored within a routing information base. BGP can access this information and use it to choose the best peering option. It uses port 179.

You can use the command `router# show ip route` to check routing and see a summary by using the command `router# show ip bgp summary`.

OSPF

OSPF, or Open Shortest Path First, is a link-state routing protocol used to find the best path between the source and the destination router. It works on port number 89 and uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for updates to a designated router or backup router.

The router ID is the highest active IP address present on the router. The router priority is an 8-bit value assigned to a router operating OSPF that is used to elect the designated router (DR) and backup designated router (BDR) in a broadcast network. A DR is elected to minimize the number of adjacencies formed while a BDR is simply used when the DR goes down. The OSPF device goes through certain states including down, INIT, 2WAY, Exstart, Exchange, Loading, and Full, which are all described in source 16.

You can use the command `show ip ospf [process-id]` to display information about the OSPF routing process.

IMAP

Internet Message Access Protocol, or IMAP, allows you to receive emails from the mail server. It can manage multiple mailboxes, provide message flags to tell what's been seen, decide whether to retrieve email from a mail server, and download media when multiple files are attached.

It is a combination of client and server processes running on other computers that are connected through a network. It listens on port 143 by default, which is non-encrypted. However, you can use port 993 for an encrypted port.

IMAP Command	Description
`LOGIN`	Authenticates the user with username and password
`LIST`	Lists the available mailboxes or folders on the server
`SELECT`	Selects a mailbox or folder on the server
`FETCH`	Retrieves email messages from the selected mailbox or folder
`STORE`	Modifies the attributes of email messages such as their flags or labels
`SEARCH`	Searches for email messages that match specific criteria
`UID`	Refers to email messages by their unique identifier
`EXPUNGE`	Removes messages that are marked for deletion from the mailbox permanently
`APPEND`	Adds new messages to a mailbox

SIP

SIP, or the Session Initiation Protocol, establishes sessions, manages signaling, and terminates connections when the session end. It enables Voice over Internet Protocol (VoIP) by defining

messages sent between endpoints and managing the elements of a call. It supports voice calls, video conferencing, instant messaging, and media distribution.

SIP sets up the session by sending packets between two or more identified IP endpoints (SIP addresses). Every SIP address is linked to a physical SIP client or software client. SIP does not encode, decode, or transport any information during sessions. It uses port 5060 or 5061 to connect to SIP servers and SIP endpoints. 5060 is not encrypted while 5061 is encrypted.

SIP Command	Description
`INVITE`	Invites a user to a call
`ACK`	Acknowledgement used to facilitate reliable message exchange for `INVITE`s
`BYE`	Terminates a connection between users
`CANCEL`	Terminates a request, or search, for a user; used if a client sends an INVITE and then changes its decision
`OPTIONS`	Solicits information about a server's capabilities
`REGISTER`	Registers a user's current location
`INFO`	Used for mid-session signaling

SMB

The Server Message Block Protocol (SMB) is used for sharing access to files, printers, serial ports, and data on a network. It can carry transaction protocols for authenticated inter-process communication.

It works through a client-server approach. A client makes specific requests and the server responds (AKA a response-request protocol). It facilitates file shares between networked computers. A user of the application can open, read, move, create, and update files on the remote server once connected. It has run using IP on port 139 and UDP on ports 137 and 138. Now it typically uses port 445.

SNMP

SNMP, or the Simple Network Management Protocol, is used to monitor and manage network devices that are connected over an IP. It's used for communication between routers, switches, firewalls, load balancers, servers, and wireless devices. It collects, organizes, and sends data from various devices for network monitoring.

Monitored endpoints and the monitoring system rely on SNMP for seamless communication. SNMP uses both ports 161 and 162 to send commands and messages. SNMP monitoring tools

help automatically discover, monitor, and manage network devices while monitoring key performance metrics at device and interface levels. It also allows you to configure threshold limits and generate alerts for anomalies.

It works by sending protocol data units (SNMP GET requests) to network devices that respond to SNMP. Monitoring tools then use GET requests to fetch data from SNMP. SNMP consists of an SNMP manager, managed devices, SNMP agent, and SNMP management information base (MIB) files, and SNMP object identifiers (OIDs). For more information, refer to source 21.

You can start SNMP by using the command `snmpstart`. `snmpget` retrieves the value of a MIB object while `snmpset` sets the value of a MIB object. `snmpsync` sends any existing GET, GETNEXT, and SET PDUs. `snmpend` terminates the session.

Sources

1. What is the Remote Desktop Protocol (RDP)?
2. How to use Remote Desktop
3. What is FTPS?
4. SSH File Transfer Protocol (SFTP): Get SFTP client & server
5. Using SFTP for Remote File Transfer from the Command Line
6. Understanding Post Office Protocol (POP3)
7. What is HTTP?
8. What is HTTPS?
9. What is DNS (Domain Name System)?
10. What is Address Resolution Protocol (ARP)?
11. What is Spanning Tree Protocol - STP
12. What is Network Time Protocol? Why Is It Important?
13. What is IGMP? | Internet Group Management Protocol
14. Simple Mail Transfer Protocol (SMTP)
15. What is Border Gateway Protocol (BGP)?
16. Open Shortest Path First (OSPF) protocol States
17. Internet Message Access Protocol (IMAP)
18. Session Initiation Protocol (SIP)
19. What Is the SIP Protocol?
20. What is an SMB Port? A Detailed Description of Ports 445 + 139
21. What is SNMP?
22. Concepts and Configuration of the Spanning Tree Protocol
23. Commands of SIP

24. SNMP commands