BERITECK

HTTP METHODS

WHAT IS AN HTTP METHOD?

BERITECK

* HTTP (Hypertext Transfer Protocol) methods are a set of request methods used by clients to request resources from servers.

* These methods indicate the desired action to be performed on the resource.

GET

BERITECK

Requests a representation of the specified resource.

GET requests should only retrieve data and should not have any other effect.

EX: *Visit google.com, Netflix.com, Beriteck.com*

POST

BERITECK

Submits data to be processed to the specified resource. POST requests can change the state of the server or trigger some action.

EX: Login to a site with *username* and *password*

PUT

BERITECK

Updates the specified resource with the request payload. PUT requests are idempotent, meaning that multiple identical requests should have the same effect as a single request.

EX: upload a picture to a site

DELETE

BERITECK

Deletes the specified resource.

EX: Delete an uploaded file/picture.

HEAD

BERITECK

Requests the headers of the specified resource without the body content.

OPTIONS

BERITECK

Returns the HTTP methods that the server supports for the specified URL

BERITECK

WIRESHARK

WHAT IS WIRESHARK

BERITECK

Wireshark is a popular open-source network protocol analyzer. It is used for capturing and analyzing network traffic in real-time or from saved capture files.

IMPORTANCE

BERITECK

Wireshark is a powerful tool that helps:

network administrators,

security professionals,

developers

to **understand what is happening on their network**, troubleshoot network issues, and investigate security incidents.

TYPES OF FILTER

BERITECK

- Display filter (What you want to see from the results)
- Capture filter (what you want to intercept)

CLI CAPTURE

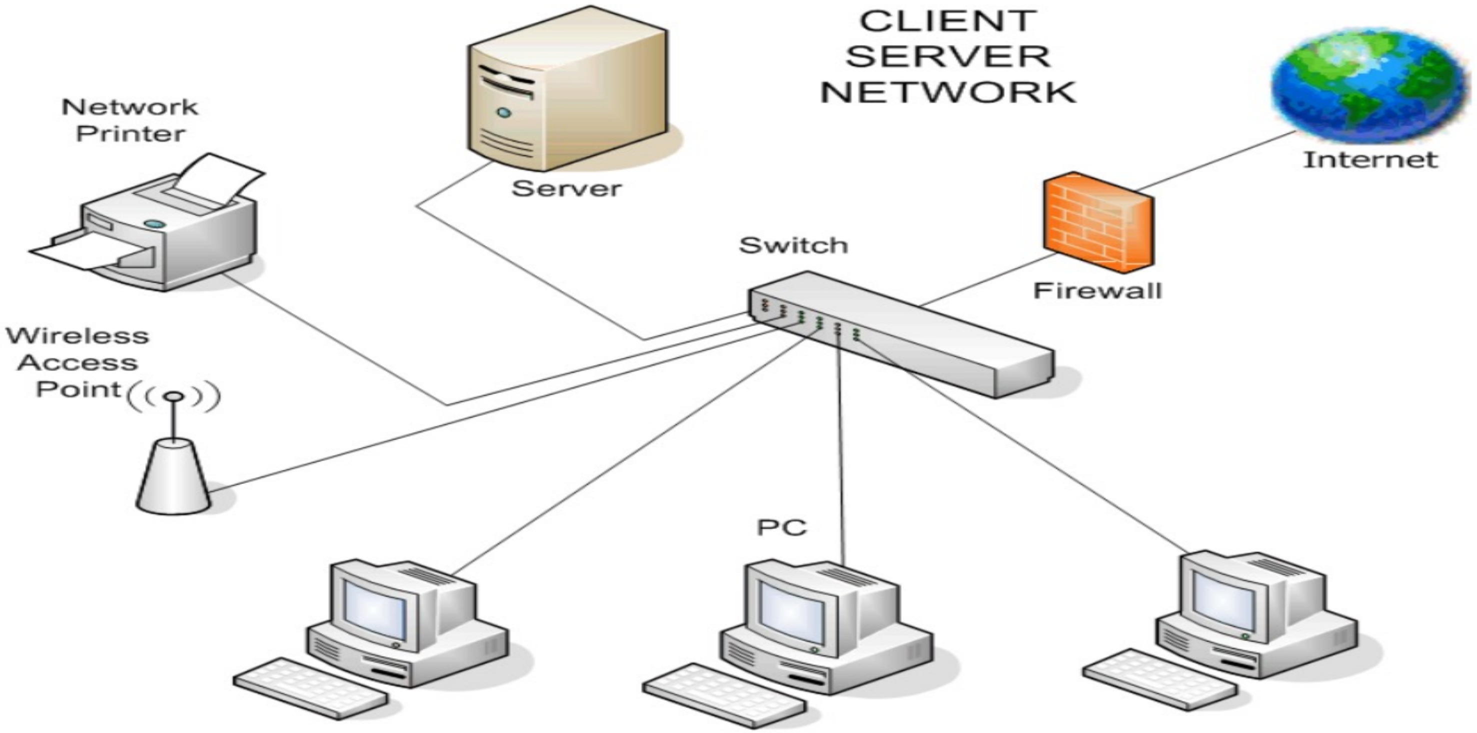
BERITECK

Network packets can also be captured using CLI tools like:

- Tshark
- TCPdump
- Dumpcap

WHERE SHOULD WIRESHARK BE PLACED IN A NETWORK?

BERITECK



DESCRIBE THE WIRESHARK INTERFACE

BERITECK

- Display filters VS capture filters

- Interfaces to capture traffic on

- Wireshark profiles

- Menu Bar

*File,

*Edit “preferences”

*View ”coloring rules”

*Statistics

FOLLOW “TCP STREAM”

BERITECK

The "Follow TCP Stream" feature in Wireshark serves the purpose of providing a ***consolidated view of the entire communication between two endpoints*** over a TCP (Transmission Control Protocol) connection.

It allows you to see the complete exchange of data between the sender and receiver in a more human-readable format.

BERITECK

DEMO TIME

CHALLENGE 101

BERITECK

* Three-way handshake

* Observe a Redirect (HTTP 302)

FTP-CLIENTSIDE 101

BERITECK

* Three-way handshake

* FTP Username and Password

* Extract Images (pantheon.jpg)

* Frame 5851 (file sent)

HTTP-BANKING

HTTP://DEMO.T3-FRAMEWORK.ORG/JOOMLA30/INDEX.PHP/EN/JOOMLA-PAGES/SAMPLE-PAGE-2/LOGIN-PAGE

BERITECK

- Visit the site above and intercept the traffic
- Filter the traffic on HTTP
- Check the credentials from POST request
- Export object (HTTP)
- Visit any https site and login then show encrypted data

HTTP-DISNEY

BERITECK

- multiple DNS request to www.disney.com
- Packet 16 shows a redirect (301)
- Packet 38 – 46 (multiple DNS requests to other sites
- Observe the server initiates connection termination
- visit who.is