God Of Protocol

**Telnet**

**Telnet** (short for "teletype network")[[1]](https://en.wikipedia.org/wiki/Telnet#cite_note-:0-1)[[2]](https://en.wikipedia.org/wiki/Telnet#cite_note-:1-2) is a [client/server](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) [application protocol](https://en.wikipedia.org/wiki/Application_layer) that provides access to virtual [terminals](https://en.wikipedia.org/wiki/Computer_terminal) of [remote systems](https://en.wikipedia.org/wiki/Remote_system) on [local area networks](https://en.wikipedia.org/wiki/Local_area_network) or the [Internet](https://en.wikipedia.org/wiki/Internet).

**PunyCode:**"Punycode is a way of converting words that cannot be written in ASCII, into a Unicode ASCII encoding."

What is an Intrusion Detection System?

An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system. Some IDS’s are capable of responding to detected intrusion upon discovery. These are classified as intrusion prevention systems (IPS).

**Network intrusion detection systems (NIDS):** A system that analyzes incoming network traffic.

**Host-based intrusion detection systems (HIDS):** A system that monitors important operating system files.

 IDS types:

**Signature-based & Anomaly-based**

Anomaly-based work behavioral with machinelearning help

**What are different kind of HTTP Requests ?**

There are several types of HTTP requests used in web communication. Here are the main ones:

1. GET: The GET request is used to retrieve or fetch a resource from a server. It sends a request for a specific resource identified by a URL. GET requests are considered “safe” as they should not have any side effects on the server.

2. POST: The POST request is used to submit data to be processed by a server. It sends data in the body of the request to a specific URL. POST requests can have side effects on the server, such as creating a new resource or updating existing data.

3. PUT: The PUT request is used to upload or replace a resource at a specific URL. It sends data in the body of the request to the server, overwriting the existing resource if it already exists.

4. DELETE: The DELETE request is used to delete a specific resource identified by a URL. It sends a request to remove the resource from the server.

5. PATCH: The PATCH request is used to partially update a resource. It sends data in the body of the request to modify specific fields or properties of an existing resource.

6. HEAD: The HEAD request is similar to a GET request but only retrieves the headers of the response, without the actual content. It is often used to check the status or metadata of a resource without downloading the entire payload.

7. OPTIONS: The OPTIONS request is used to retrieve the communication options available for a given resource or server. It helps determine which HTTP methods and headers are supported by the server.

8. TRACE: The TRACE request is used to perform a loopback test by having the server return the received request back to the client. It can be used for debugging or diagnostics purposes.

9. CONNECT: The CONNECT request is used to establish a network connection to a server over a proxy. It is commonly used for setting up secure communication through HTTPS.

Link of good article about ARP:  
[**https://www.fortinet.com/resources/cyberglossary/what-is-arp**](https://www.fortinet.com/resources/cyberglossary/what-is-arp)

difference between IPv4 and IPv6 header:

[**https://dev.to/codexam/what-is-the-difference-between-ipv4-and-ipv6-packet-format-3315**](https://dev.to/codexam/what-is-the-difference-between-ipv4-and-ipv6-packet-format-3315)

**IPv4 🡪 IP Private Range** **:**

10.0.0.0 / /8 🡪 ( 10.0.0.1 to 10.255.255.254 )

172.16.0.0 / /12 🡪 ( 172.16.0.1 to 172.31.255.254 )

192.168.0.0 / /16 🡪 ( 192.168.0.1 to 192.168.255.254 )

Best document about **Address**

**“Allocation for Private Internets” :**

https://datatracker.ietf.org/doc/html/rfc1918

**What is Handle ID** (chat)

In Windows security logs, particularly those related to system and security events, a "Handle ID" refers to a unique identifier assigned to a specific handle when a process or thread opens a handle to an object, such as a file, registry key, or process.

### What is a Handle?

A handle in the Windows operating system is an abstract reference to a system resource. Handles are used by applications to manage resources like files, registry keys, processes, threads, or network connections.

### Handle ID in Logs

When you see a "Handle ID" in a log entry, it typically represents the specific handle that was used by the operating system or an application to access or manipulate a particular resource. This ID is unique for the duration that the handle is open.

### Where You Might See Handle ID:

- \*\*Windows Security Logs:\*\* For example, in event ID 4656 ("A handle to an object was requested") or 4663 ("An attempt was made to access an object"), the Handle ID is logged to help track which handle was used to perform the operation.

- \*\*Sysmon Logs:\*\* If you're using Sysmon, you might see Handle ID information in events related to process creation, file creation, or other actions that involve system handles.

### Example Use Case:

- \*\*Tracking Access:\*\* If an unauthorized access attempt occurs, the Handle ID helps correlate the specific handle used during the operation. This can assist in forensic investigations to trace which process opened the handle and what actions were performed with it.

### Why is Handle ID Important?

- \*\*Auditing:\*\* Handle IDs are important in security auditing because they allow administrators to track which handles are being used by specific processes. This can help in identifying unauthorized access or misuse of system resources.

- \*\*Forensics:\*\* In a forensic investigation, Handle ID helps correlate events and operations performed by processes, providing insights into how a potential compromise or malicious activity occurred.

In summary, the Handle ID in logs is a crucial piece of information for tracking and analyzing resource access and manipulation on a Windows system.

a Handle ID is like a "ticket number" the operating system gives to programs so they can access and manage system resources like files. The program uses this Handle ID whenever it wants to interact with the resource, and the operating system takes care of the rest, ensuring efficient and secure management of resources

**DLL Hijacking and DLL Injection**

In summary, DLL hijacking involves tricking a legitimate application into loading a malicious DLL, while DLL injection involves forcibly loading a DLL into a target process to execute arbitrary code.

* **Vulnerability**: Vulnerable means susceptible to attack or damage. In information security, a vulnerability is a weakness.
* **Threat**: A threat is a potential danger associated with this weakness or vulnerability.
* **Risk**: The risk is concerned with the likelihood of a threat actor exploiting a vulnerability and the consequent impact on the business.

**Linux Auditd :**

Auditd is a Linux tool designed for monitoring and recording system events to provide a comprehensive audit trail of user activities, system changes, and security access. Auditd operates by hooking into the Linux kernel, capturing detailed information about system calls and other system events as they happen. These events are then logged to a file, providing a timestamped record. Administrators can define rules that specify which events to log, offering the flexibility to focus on specific areas of interest or concern. The logged data can be used for a variety of purposes, from compliance auditing to detailed forensic analysis.