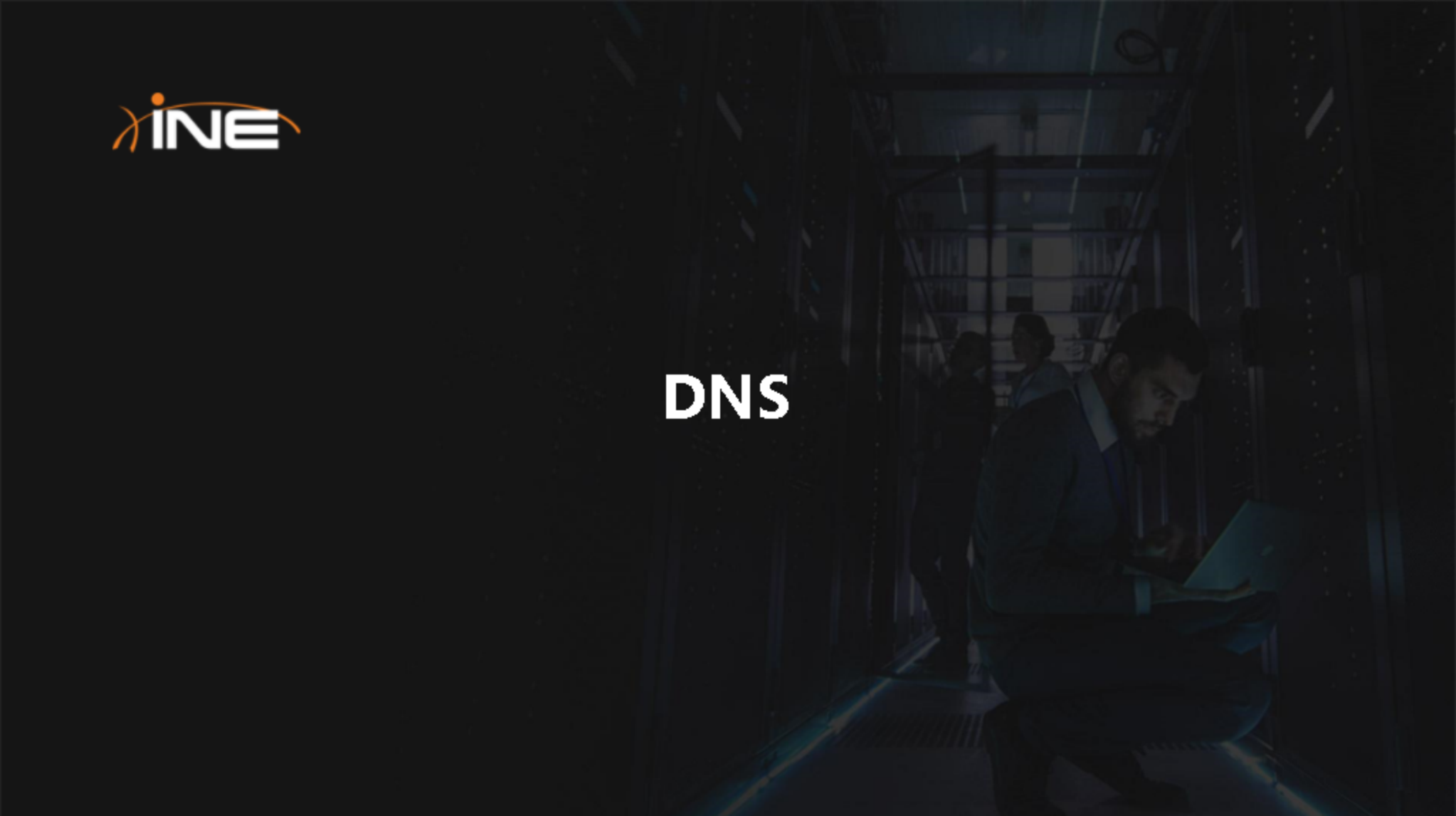
DNS



2.7 DNS

+ **How does this support my pentesting career?**

  - SSL/TLS certificates validation relies on DNS
  - Mounting spoofing attacks
  - Performing information gathering

2.7 DNS

- The **Domain Name System**, or **DNS**, is the only application layer protocol you will see in this module.

- The DNS primarily converts human-readable names, like `www.elearnsecurity.com`, to IP addresses and is a fundamental **support protocol** for the Internet and computer networks in general. It is widely recognized that the entire internet security is relying upon DNS.

2.7 DNS

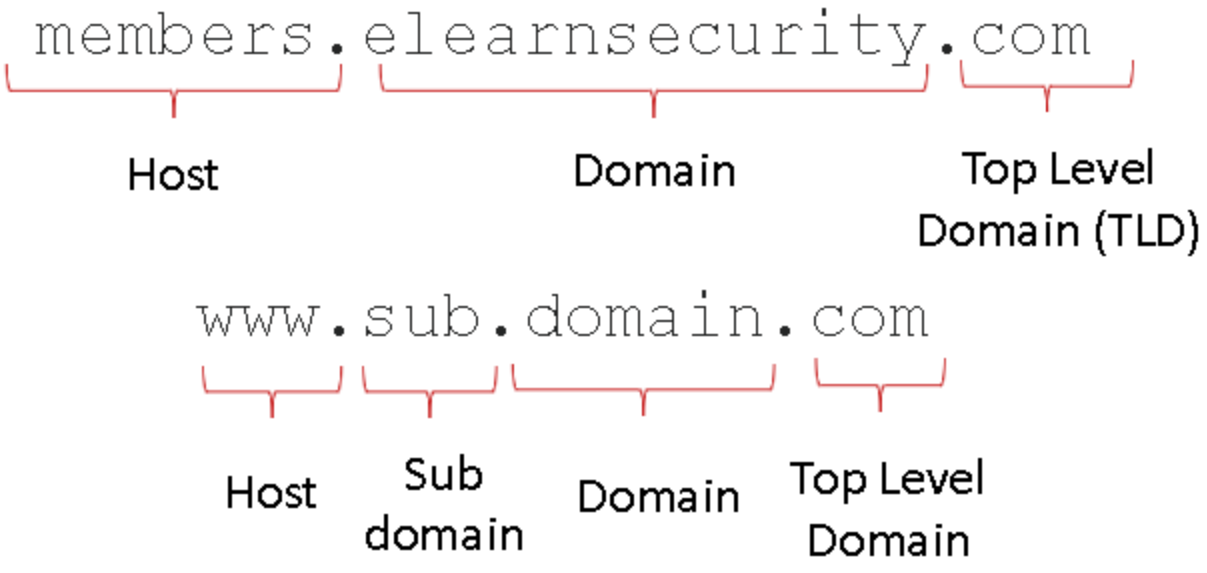
- For this course, you will need to know how the DNS service provides name resolution because every common operation on the Internet such as opening a web site, sending an email, and sharing a document involves the use of a DNS to resolve resource names to IP addresses (and vice versa).

2.7.1 DNS Structure

- A DNS name such as `www.elearnsecurity.com` or `members.elearnsecurity.com` can be broken down into the following parts:
  - Top level domain (TLD)
  - Domain part
  - Subdomain part (if applicable)
  - Host part

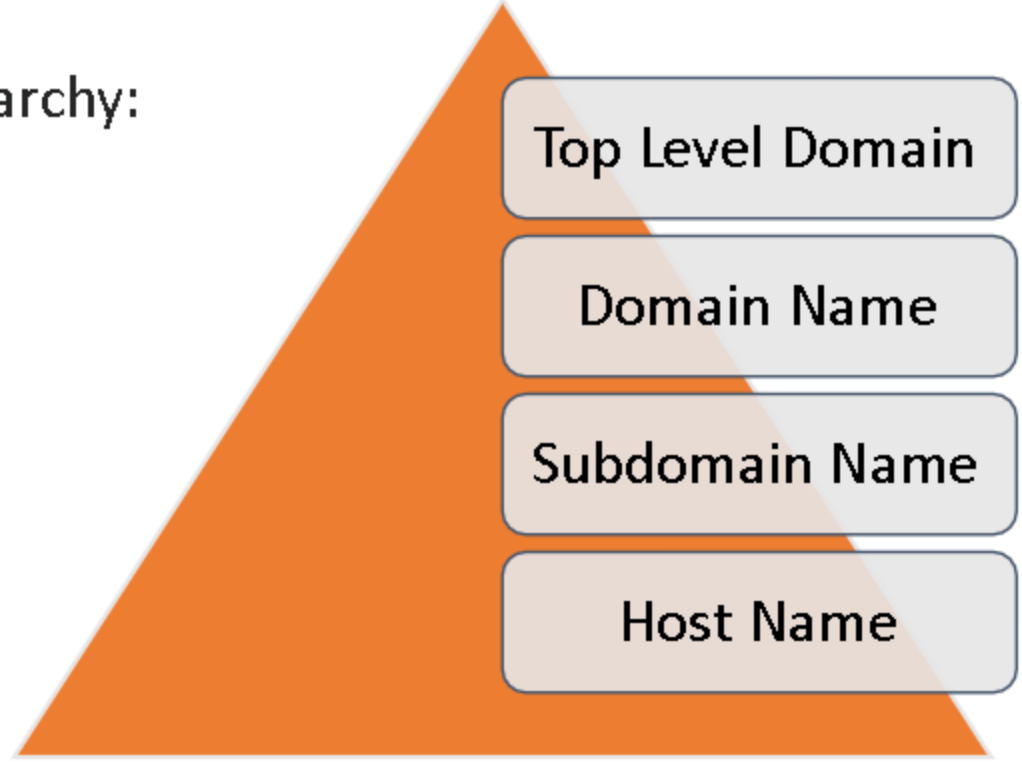
2.7.1 DNS Structure

+ **EXAMPLE**



2.7.1 DNS Structure

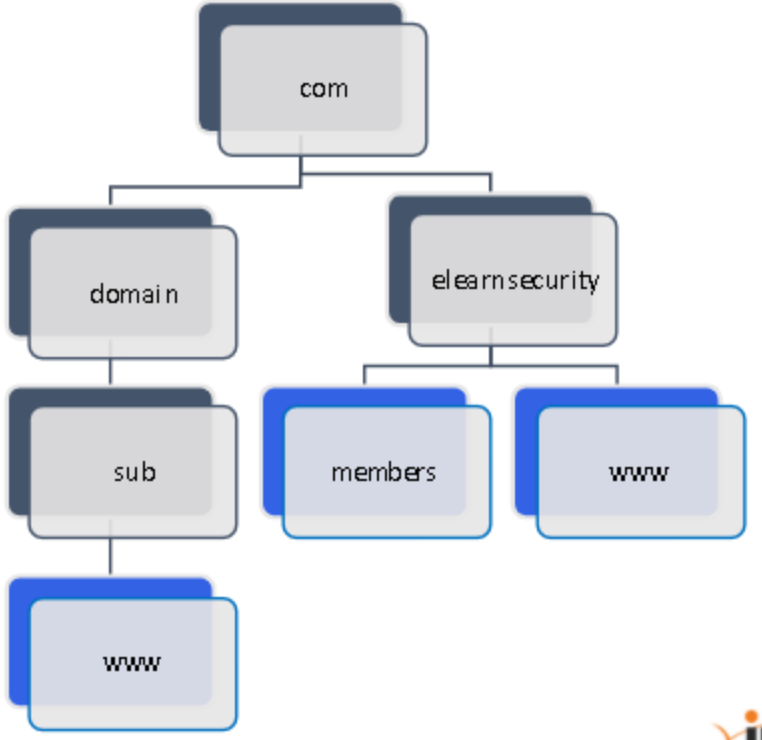
- These parts form a hierarchy:



2.7.1 DNS Structure

EXAMPLE:

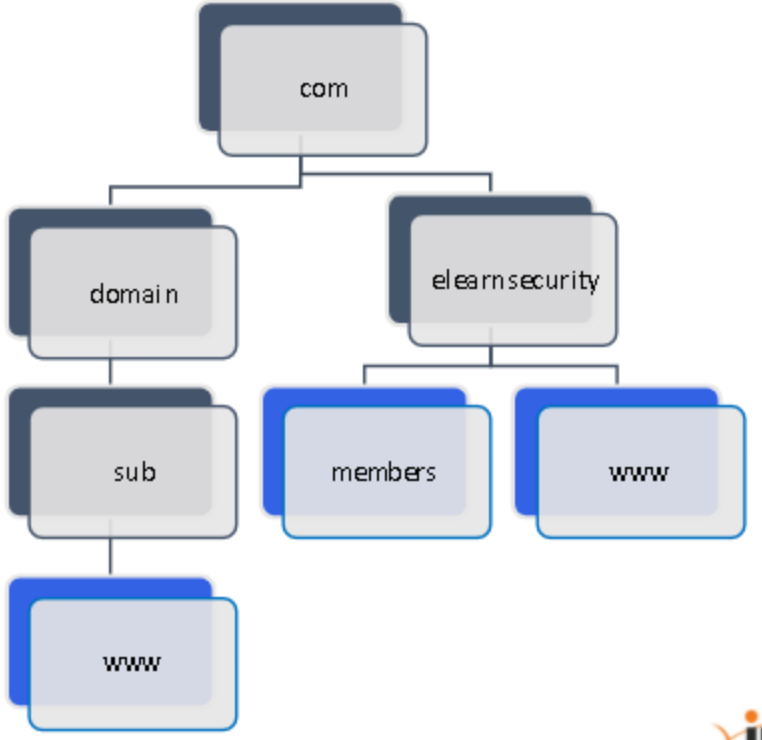
+ So, we can rewrite the previous names as:



2.7.1 DNS Structure

EXAMPLE:

+ Where the blue squares are the hosts, and the red ones are the top/sub/domain names.



2.7.1 DNS Structure

- Name resolution is performed by **resolvers**, servers that contact the top-level domain (TLD) DNS servers and follow the hierarchy of the DNS name to resolve the name of a host.

- Resolvers are DNS servers provided by your ISP or publicly available like OpenDNS or Google DNS.

2.7.2 DNS Names Resolution

- To convert a DNS name into an IP address, the operating system must contact a **resolver** server to perform the DNS resolution.
- The resolver breaks down the DNS name in its parts and uses them to convert a DNS name into an IP address.

2.7.2.1 DNS Resolution Algorithm

1. Firstly, the resolver contacts one of the **root name servers**; these servers contain information about the top-level domains.

2. Then, it asks the TLD name server what's the name server that can give information (authoritative name server) about the **domain** the resolver is looking for.

3. If there are one or more **subdomains**, step 2 is performed again on the authoritative DNS server for every subdomain

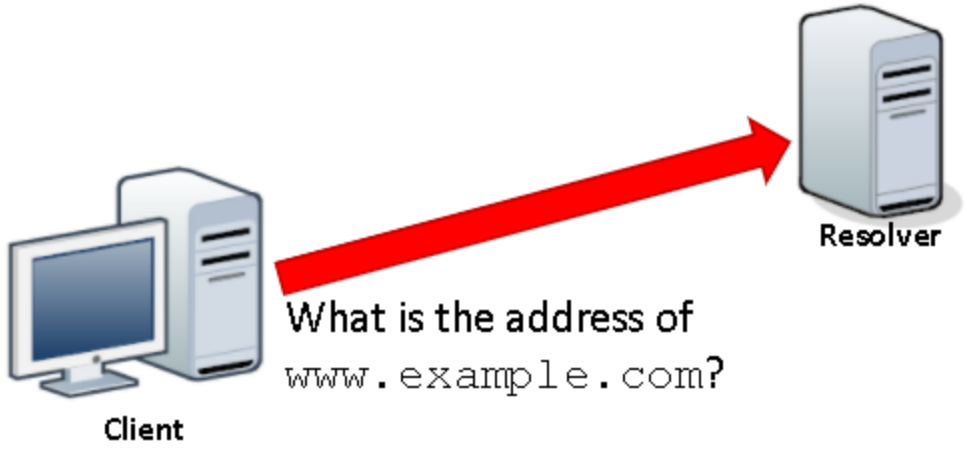
4. Finally, the resolver asks for the name resolution of the **host** part.

2.7.2.2 DNS Resolution Example

- A computer needs to open a web page on `www.example.com`.

2.7.2.2 DNS Resolution Example

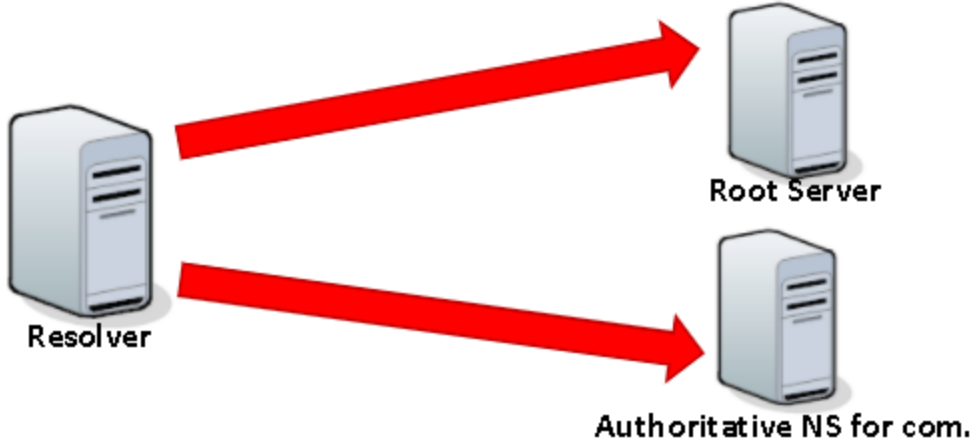
+ To do that, it contacts the resolver configured by the local administrator (e.g., OpenDNS).



2.7.2.2 DNS Resolution Example

- The resolver contacts a **root server** and asks about the authoritative name server(s) for the `com.` domain.

- Then the resolver contacts that authoritative name server and asks what is an authoritative name server for the `example.com.` domain.



2.7.2.2 DNS Resolution Example

- The resolver then asks what the address of www is.
- Finally, the resolver sends the IP address back to the client.

2.7.3 Resolvers and Root Servers

- How can a resolver know how to contact a **root name server**?
- IP addresses of the root servers are **hardcoded in the configuration** of the resolver. System administrators keep the list updated, otherwise, the resolver would not be able to contact a root server!

2.7.4 Reverse DNS Resolution

- The domain name system can also perform the inverse operation; it can convert an **IP address to a DNS name.**

- Keep in mind that this is not always the case; the administrator of a domain must have enabled and configured this feature for the domain to make it work.

2.7.4 Reverse DNS Resolution

EXAMPLE

+ Many tools use the reverse DNS if it's available.

+ The Linux ping utility performs a reverse DNS query after receiving every response from the target.

```
$ ping www.yahoo.com
PING fd-fp3.wg1.b.yahoo.com (46.228.47.115) 56(84) bytes of data.
64 bytes from ir1.fp.vip.ir2.yahoo.com (46.228.47.115): icmp_req=1 ttl=49 time=125 ms


--- fd-fp3.wg1.b.yahoo.com ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1001ms
rtt min/avg/max/mdev = 125.706/125.706/125.706/0.000 ms
```

2.7.5 More about the DNS

- In this section, you have seen how the DNS is used to perform name resolution. The domain name system is not just that, it is used to identify what the mail servers for a domain are, to know what is the right server for a specific role and much more.

- Please refer to RFC1034 and RFC1035 to dig more into DNS!

- *NOTE: the DNS is also very important to the security of the whole internet because breaking DNS security means breaking SSL and TLS. This, however, is beyond the scope of this training course.*

https://www.ietf.org/rfc/rfc1034.txt
https://www.ietf.org/rfc/rfc1035.txt

References

- RFC1034: https://www.ietf.org/rfc/rfc1034.txt
- RFC1035: https://www.ietf.org/rfc/rfc1035.txt