Enumeration

Increasing attack vectors. Decreasing the path gives the right direction.

- The attacker creates an active connection to the system and performs directed queries to gain more info about the target.
- Attackers establish an active connection with the victim and discover as many attack vectors as possible.
- Enumeration techniques are conducted in an intranet environment.
- Scanning is finding an attack surface, enumeration is expanding it.
- Enumeration is the key to a successful penetration test.

Information enumerated by Intruders:

- Network resources
- Network shares
- Routing tables

Enumeration Techniques:

- Extract user names using email IDs
- Extract information using the default passwords

- Audit and service settings
- SNMP and DNS details
- Machine names
- Users and Groups
- Application and banners

passwords
- Extract user names using SNMP
- Brute force Active Directory
- Extract user groups from Windows
- Extract information using DNS Zone Transfer

▼ Services and Ports to Enumerate

- TCP/UDP **53**: DNS Zone Transfer
- TCP/UDP **135**: Microsoft RPC Endpoint Mapper
- UDP **137**: NetBIOS Name Service (NBNS)
- TCP **139**: NetBIOS Session Service (SMB over NetBIOS)
- TCP/UDP **445**: SMB over TCP (Direct Host)
- UDP **161**: Simple Network Management Protocol (SNMP)
- TCP/UDP **389**: Lightweight Directory Access Protocol (LDAP)
- TCP/UDP **3268**: Global Catalog Service
- TCP **25**: Simple Mail Transfer Protocol (SMTP)
- TCP/UDP **162**: SNMP Trap

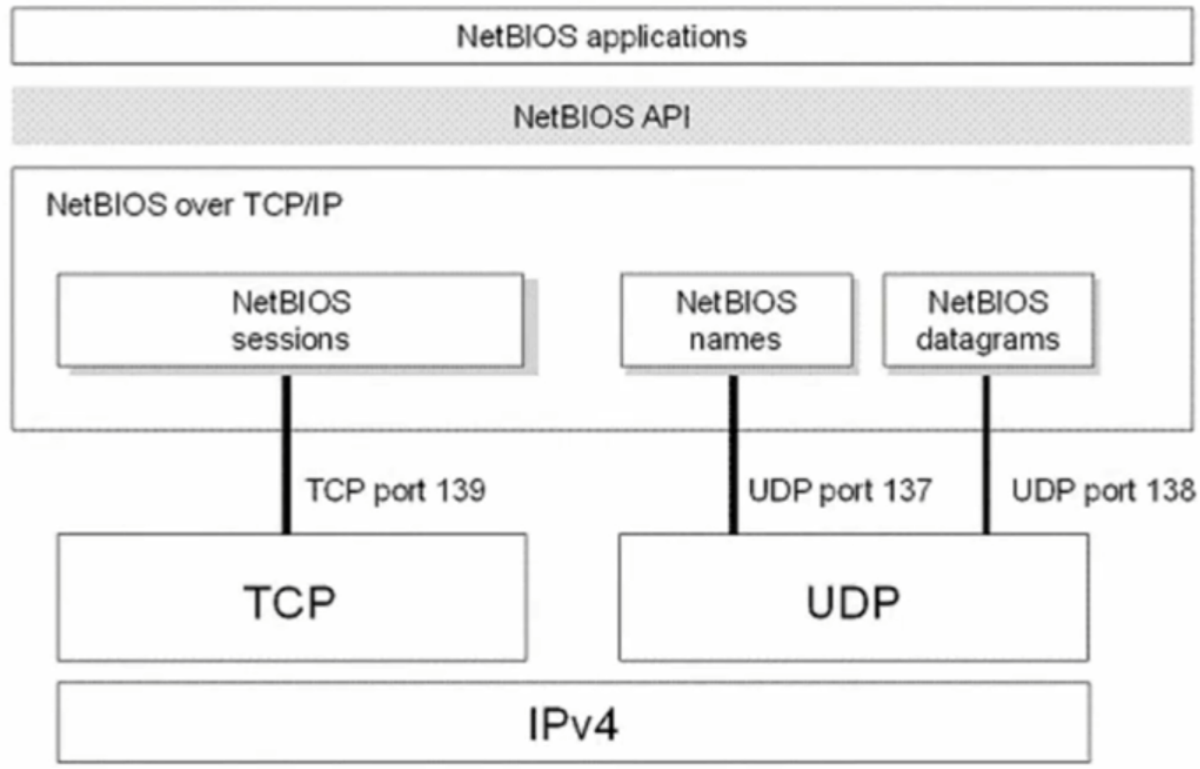
---

1. 🔛NetBIOS Enumeration

- NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network(LAN).
- Created by IBM, adopted by Microsoft

- NetBIOS is basically an API via Microsoft to share Windows information.

  Information from Windows is passed to NetBIOS API and that data is transferred to TCP/IP packets, further circulating on the network.
- NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP, 15 characters are used for the device name, and the 16th character is reserved for the service or name record type.
- Software applications on a NetBIOS network locate and identify each other via their NetBIOS name.
- Applications on other computer access NetBIOS names over UDP(NBNS).
- NetBIOS used 3 ports (137, 138, 139) 138 sending datagram packets for connectionless service UDP.
- Two applications start a NetBIOS session when the client sends a command to “call” another client (the server) over TCP port 139. (session mode).
- The “hand-up” command terminates a NetBIOS session.
- NOTE: NetBIOS name resolution is not supported by Microsoft for Internet Protocol version 6 (IPV6).



> **An attacker uses the NetBIOS enumeration to obtain:**

- List of computers that belong to Domain.
- List of shares on the individual hosts in the network.
- Policies and passwords

> **Using NetBIOS enumeration he can perform:**

- Read/Write to a shared resource depending on the availability of shares
- Launch DOS on the target
- Enumerate password policies

🛠️ Tools:

- Nbstat

It is Utility tool in Windows to display NetBIOS over TCP/IP(NetBT) protocol statistics, NetBIOS name table for both the local and remote computers, and NetBIOS name cache.

```
nbstat.exe -c
```

- Get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP address.

```
nbstat.exe -a IPaddress_of_remote_machine
```

- Gets the NetBIOS name table of a remote computer.

---

2. 🖨️SMB Enumeration

- SMB stands for Server Message Block used for sharing resources like files, printers, and any resources that should be retrievable or made available by the server.
- It runs on port 445 or port 139 (NetBIOS) depending on the server, natively available in Windows.
- To make it work for Linux, you need to install a samba server because Linux natively does not use SMB protocol.
- Operates on Layer 7, and uses TCP/IP on 445 for transport.

▼ SMB Implementation

CIFS, Samba, NQ, MoSMB, Tuxera SMB

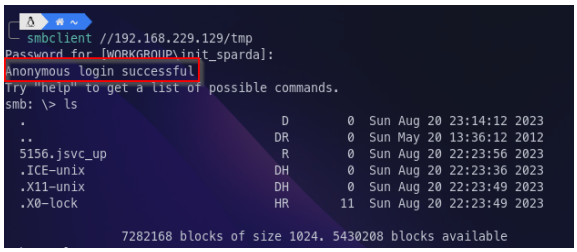
> SMB used either IP port 139 or 445

- Port 139: SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network.
- Port 445: Later version of SMB (After Windows 2000) began to use 445 on top of the TCP stack. Using TCP allows SMB to work over the internet.

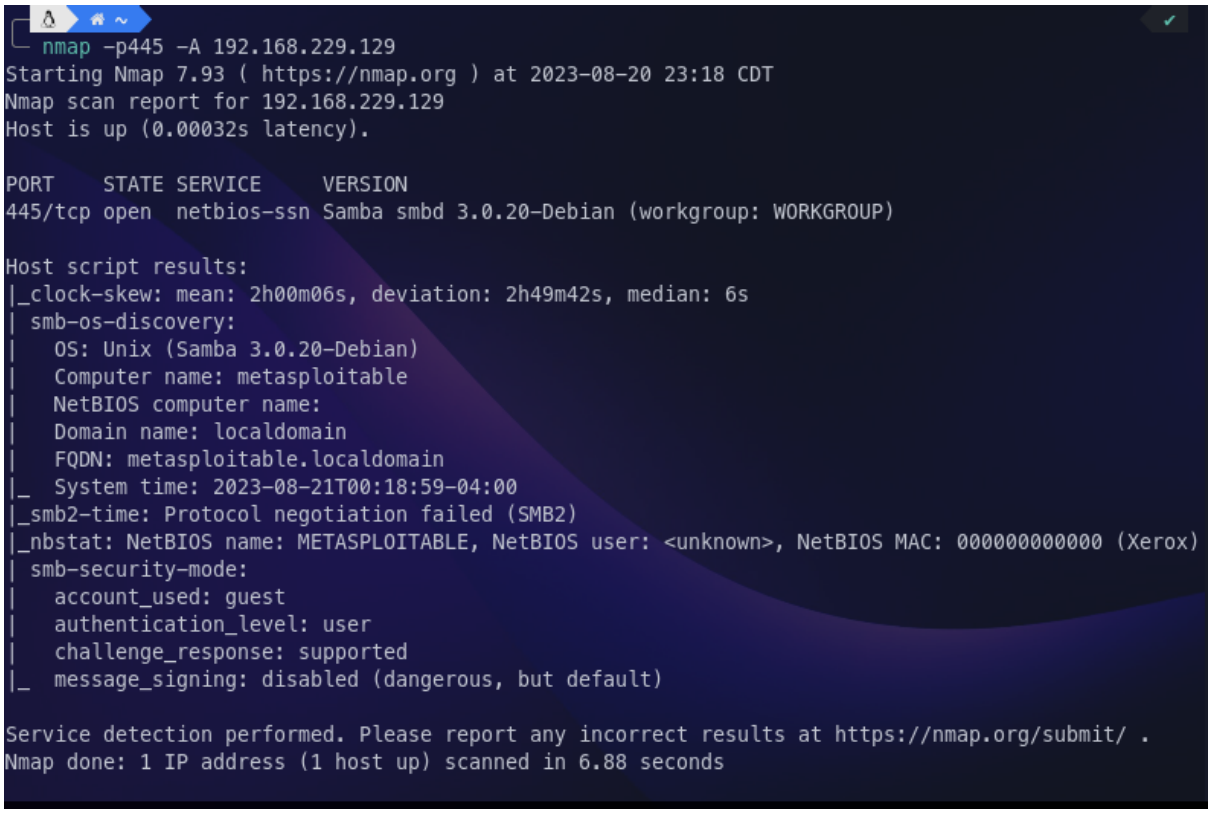
🛠️ Tools:

- smbclient
- smbman
- Nmap

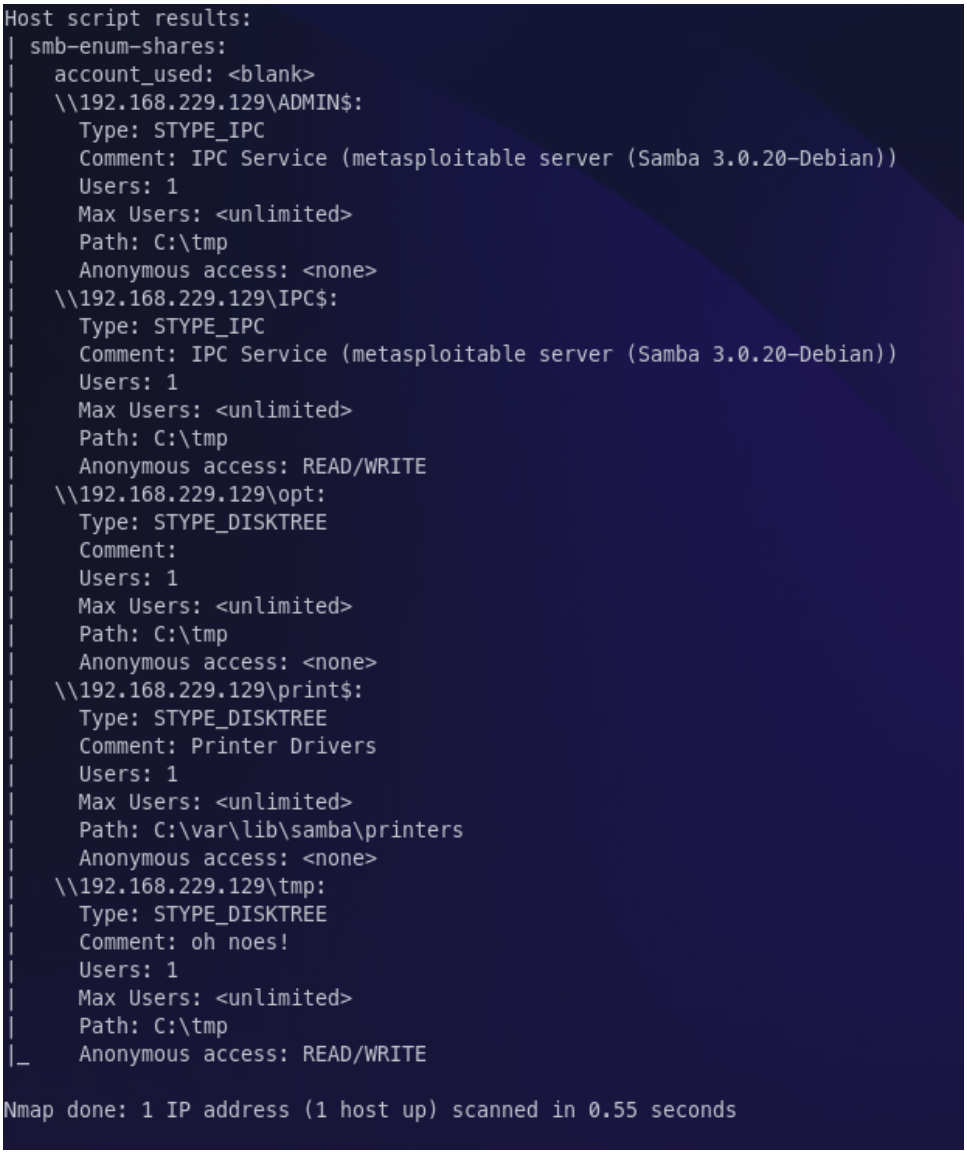
SMBCLIENT



Nmap




```
nmap –script=smb-enum-shares IPaddr
```



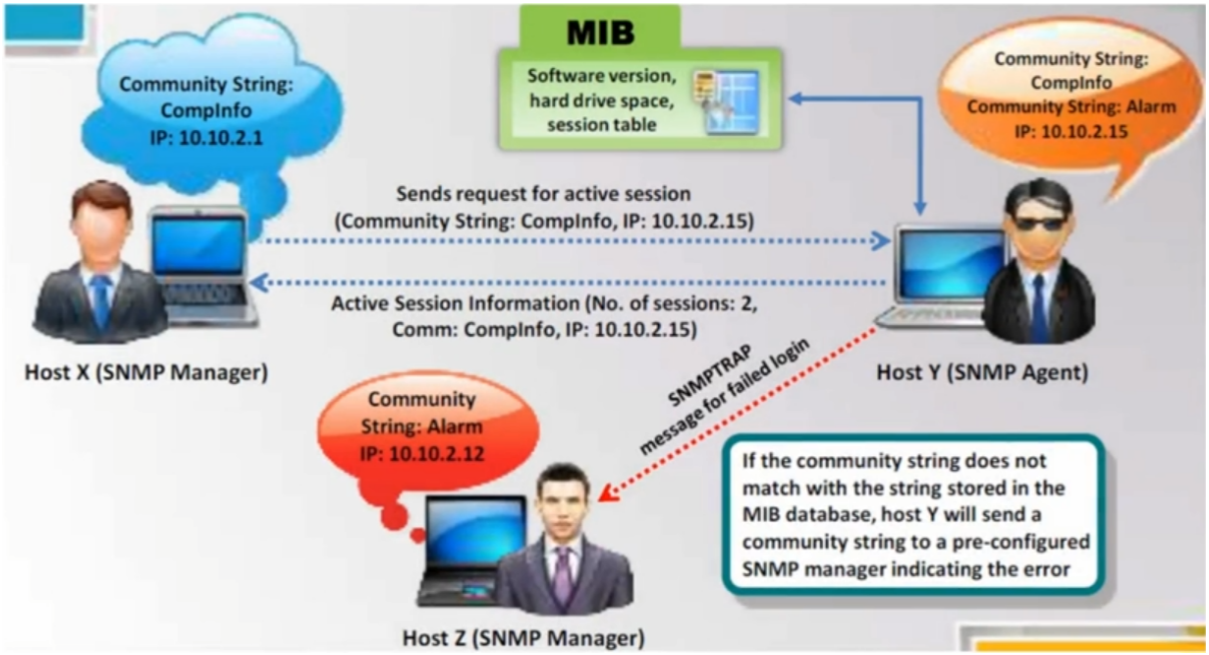
3. 👨‍💼SNMP Enumeration

- Simple Network Management Protocol is an application layer protocol that uses UCP to maintain and manage routers, hubs and switches, and other network devices on an IP network.
- SNMP enumeration is used to enumerate and gather information on user accounts, passwords, groups, system names, and devices on a target system.
- SNMP consists of a manager and an agent. Two parties
  - Agents are embedded in every network device

- A manager is installed on a separate computer

Components of SNMP:

- Managed Device: A managed device is a device or host which has the SNMP service enabled. These devices could be routers, switches, hubs, bridges, computers, etc.
- Agent: An agent can be thought of as a piece of software that runs on the managed device. Its primary job is to convert the information into SNMP-compatible format for smoother management of the network using SNMP protocol.
- Network Management System: These are the software used to monitor network devices.



▼ SNMP holds two passwords to access and configure the SNMP agent from the management station:

- Read community string: It is public by default and allows viewing of device/sys configuration.
- Read/Write community string: It is private by default and allows remote editing of configuration.

The attacker uses these default strings or brute-forcing to extract information about a device and information about

network resources such as hosts, routers, devices, shares, etc., and ARP tables, routing tables, traffic, etc.

Management Information Base (MIB)

- MIB is a virtual database containing a formal description of all the network objects that can be managed using SNMP.
- The MIB database is hierarchical and each managed object in a MIB is addressed through Object Identifier(OIDs).
- Two types of managed objects exist:
  - Scalar objects that define a single object instance.
  - Tabular objects that define multiple related object instances are grouped in MIB tables.

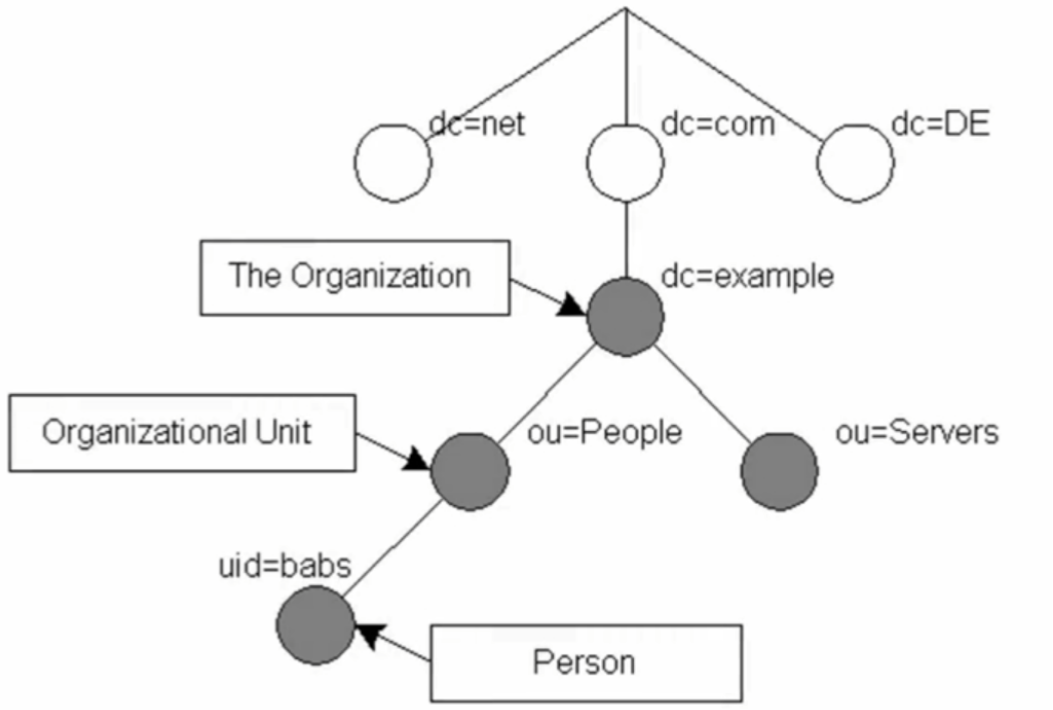
---

4. 📂LDAP Enumeration

- A lightweight Directory Access Protocol is an internet protocol for accessing distributed directory services.
- Is a Hierarchical compilation used to access directory listings within Active Directory or from other Directory Services.
- An LDAP session is established by the client by connecting Directory System Agent (DSA) on TCP port 389 and sending an operation request to the DSA. Then receives encoded information (not Encrypted)from DSA and LDAPS all data are transmitted in plain text form.
- Information is transmitted between the client and server using Basic Encoding Rules (BER).
- Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks.

Attribute	Field	Usage
CN	Common Name	Identifies the person or object.
OU	Organizational Unit	A unit or department within the organization.
O	Organization	The name of the organization.
L	Locality	Usually a city or area.
ST	State	A state, province, or county within a country.
C	Country	The country's 2-character ISO code (such as c=US or c=GB).
DC	Domain Component	Components of the object's domain.

Hierarchical Structure



5. 📧SMTP Enumeration

- A simple Mail Transfer Protocol is used to send emails to local or remote mail servers.
  - To receive mail either POP of IMAP are used.
- SMTP provides 3 built-in commands:

    - VRFY: Valid users
    - EXPN: Tells the actual delivery addresses of aliases and mailing lists
    - RCPT: Defines the recipients of the message
- SMTP servers respond differently to VRFY, EXPN, RCPT if invalid users when enumeration.
- Attackers can directly interact with SMTP via telnet prompt and collect a list of valid users on the SMTP server.

> 🛠️ Tools:
>
> - smtp
> - Metasploit

---

6. 🌐DNS Enumeration (Zone transfer)

- It is a process of locating the DNS server and records of the target network.
- An attacker can gather information such as the DNS server name, hostname, machine names, username, and IP address of potential targets.
- The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses.
- In DNS zone transfer enumeration, the attacker tries to retrieve a copy of the entire zone file for a domain from the DNS server.

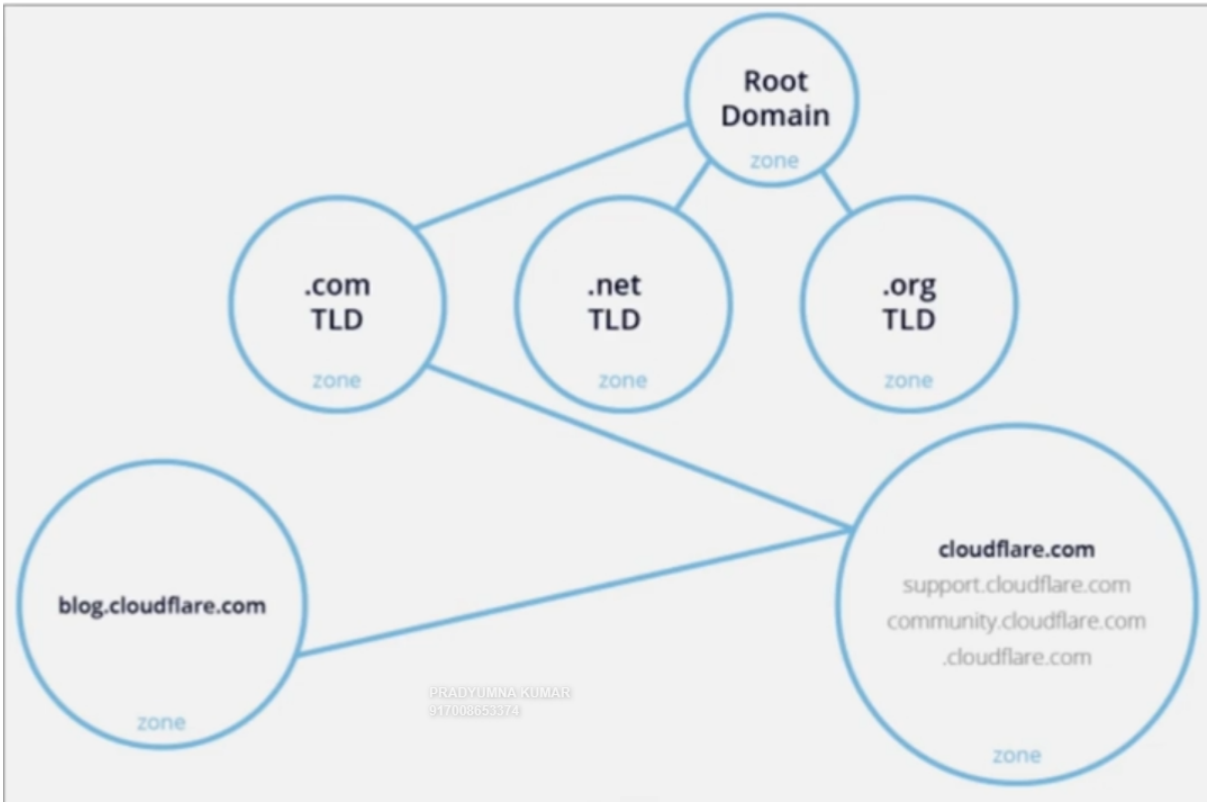
DNS Zone

- It is a portion of the DNS namespace that is managed by a specific organization or administrator.
- It is an administrative space that allows for more managed/granular control of DNS components, such as an

authoritative name server.

    - Granular control changes in the smallest level by separating them with different types of records for faster search.

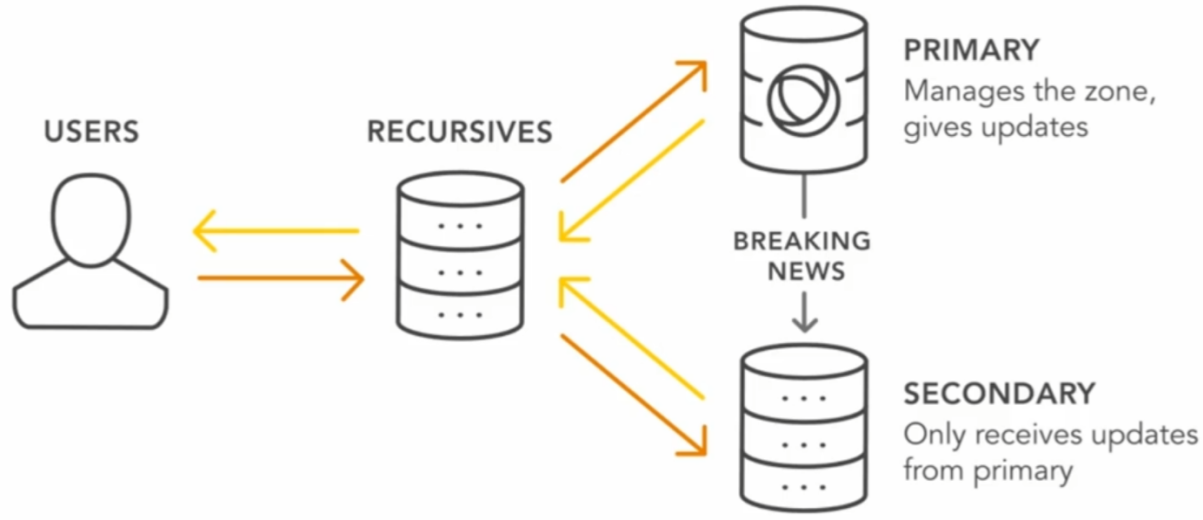
- In face, a DNS can contain multiple subdomains and multiple zones can exist on the same server.
- DNS zone are not necessarily physically separated from one another, zones are strictly used for delegating control.



- All the information for a zone is stored in DNS zone file, the key to understanding zone operation.
- A zone file is a plain text file stored in DNS server that contains an actual representation of zone and contains all the records for every domain within zone.
- Zone file must always start with a Start of Authority record, which contains important information including contact information for the zone administrator.

Zone Transfer

- A primary DNS server only has the master copy of the zone, and a secondary DNS will have a copy of zone for redundancy.
- Whenever there is a change in the zone data on the primary DNS, then the changes have to be shared to the secondary DNS of the zone. This is Zone Transfer.
- A zone transfer uses the TCP for transport and takes the form of a client-server transaction.



- Zone transfers are automatically triggered when the zone serial number increments (the number increases). The zone serial number increments when the zone receives an update.
- A zone transfer can be full or incremental.
  - Full zone transfers are referred to as AXFR (Asynchronous full transfer or authoritative full transfer)
  - Incremental zone transfers are IXFR (Incremental transfer)
- AXFR offers no authentication, so any client can ask a DNS server for a copy of the entire zone.
- This means that unless some kind of protection is introduced, an attacker can get a list of all hosts for a domain, which gives them a lot of potential attack vectors.

🛠️ Tools:

- host
- nslookup
- dig

host:

```
host -t ns zonetransfer.me
host -l zonetransfer.me name_server
```

nslookup:

- By default give A records

```
nslookup
> set type=a
> google.com

> set type=cname
> google.com
```

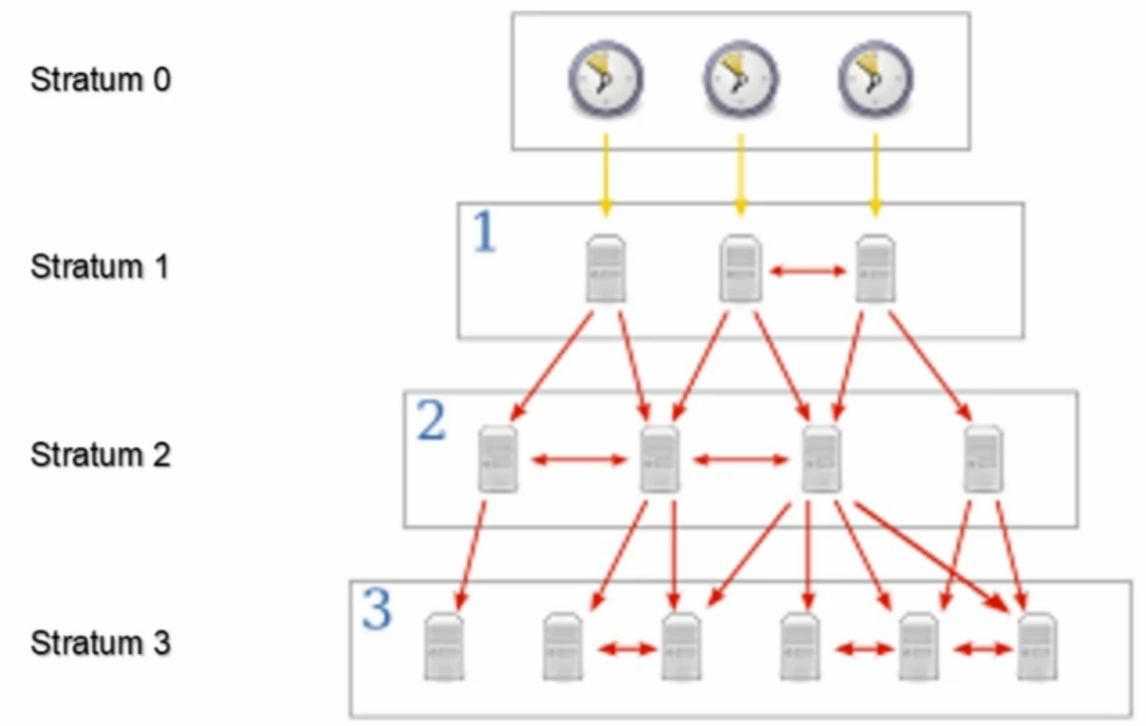
```
nslookup
> set type=ns     [ Name Server ]
> TLD
> server nsztml.digi.ninja
> set type=any
ls -d maindomain.TLD
```

dig full zone transfer:

```
dig axfr @name.serv.er domain.TLD
```

NTP Enumeration

- Network Time Protocol is designed to synchronize clocks of networked computers.
- It uses UDP port 123 as its primary means of communication.
- NTP can maintain time to within 10 millisecond (1/100 sec) over the public internet.
- It can achieve accuracies of 200 microsec or better in local area networks under ideal conditions.
- Attacker queries NTP server to gather valuable information such as:
  - List of hosts connected to NTP server
  - Clients IP addresses in a network, their system names and OSs
  - Internal IPs can also be obtained NTP server is in the DMZ



Enumeration Countermeasures

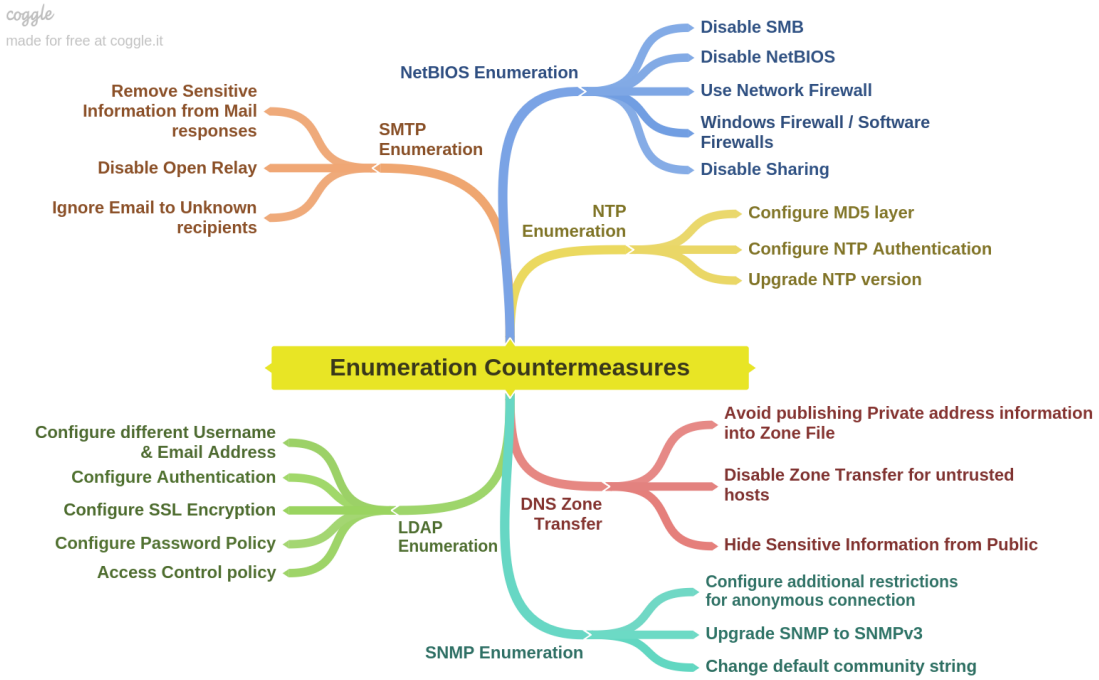
- NetBIOS:

- Disable SMB (Under Windows Features)
- Disable NetBIOS (Under Network TCP/IP setting)
- Use Network Firewall
- Use Windows/Software Firewalls
- Disable Sharing

- SNMP:
  - Remove SNMP agent(MIB is present in agent) or turn off the SNMP service
  - If shutting off SNMP is not an option, then change the default community string name
  - Upgrade to SNMP3, which encrypts passwords and messages
  - Implement the Group Policy security option called “Additional restrictions for anonymous connections”
  - Ensure that access to null session pipes, null session shares, and IPSec filtering is restricted. (Proper session should be established)
- DNS:
  - Disable DNS zone transfer to untrusted hosts
  - Make sure private hosts and IP addresses are not published into DNS zone files of public DNS server
  - Use premium DNS registration services (GoDaddy) that hide sensitive information such as HINFO from public
  - Use standard network admin contact for DNS registration in order to avoid social engineering attacks

- SMTP:
  - Configure SMTP servers to
    - Ignore email messages to unknown recipients
    - Not include sensitive mail server like location, IP, and local host information

        - Disable the open relay feature
- LDAP:
    - By default, LDAP traffic is transmitted unsecured; Use SSL technology to encrypt the traffic
    - Select a user name different from your email address and enable account lockout if a failed login attempt is made
    - Configure password policy
    - Configure access control policy
- SMB:
    - Disable SMB protocol on Web and DNS servers
    - Disable SMB protocol on internet-facing servers
    - Disable ports TCP 139 and TCP 445 used by SMB protocol
    - Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry
- NTP:
    - Configure MD5 layer (Hashing)
    - Configure NTP Authentication
    - Upgrade NTP version



Reference

https://ceh.brutef0rce.com/enumeration

DNS Enumeration:

```
<https://www.hackingarticles.in/4-ways-dns-enumeration/>

<https://securitytrails.com/blog/dns-enumeration>

<https://en.wikipedia.org/wiki/DNS_zone_transfer>
```

NetBIOS and SMB Enumeration:

```
<https://www.youtube.com/watch?v=sXqT95eIAjo>

<http://nbtenum.sourceforge.net/>

<https://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/>

<https://www.hackingarticles.in/smb-penetration-testing-port-445/>

<https://tools.kali.org/information-gathering/enum4linux>
```

SNMP Enumeration:

```
<https://www.hackingarticles.in/snmp-lab-setup-and-penetration-testing/>
```

LDAP Enumeration:

```
<https://github.com/CroweCybersecurity/ad-ldap-enum>

<https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78>

<https://n0where.net/ldap-based-active-directory-enumeration>

<https://www.hackingarticles.in/lightweight-hack-the-box-walkthrough/>

<https://www.hackingarticles.in/penetration-testing-windows-server-active-directory-us
ing-metasploit-part-1/>
```

NTP Enumeration:

```
<https://www.oreilly.com/library/view/ethical-hacking-pro/200000006A0417/N00007.html>

<https://www.zerosuniverse.com/ethical-hacking/what-is-ntp-enumeration/>

<http://www.ethicaloverflow.com/m2%20enumeration.php>

<https://nmap.org/nsedoc/scripts/ntp-info.html>
```

SMTP Enumeration:

```
<https://www.hackingarticles.in/4-ways-smtp-enumeration/>

<https://www.peerlyst.com/posts/smtp-enumeration-technique-hamza-m-hirsi>

<https://tools.kali.org/information-gathering/smtp-user-enum>

<https://nmap.org/nsedoc/scripts/smtp-enum-users.html>

<http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum>
```

Enumeration Countermeasures:

```
<http://etutorials.org/Networking/network+security+assessment/Chapter+3.+Internet+Host
+and+Network+Enumeration/3.5+Enumeration+Countermeasures/>
```

```
<http://luizfirmino.blogspot.com/2011/09/enumeration-countermeasures.html>
```