Module 7
Enumeration

Ansh Bhawnani

Enumeration Concepts

Module 7

Enumeration Concepts

- Attacker creates active connections to system and performs directed queries to gain more information about the target.
- Attacker establishes an active connection with the victim and try to discover as much 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.

Enumeration Concepts

Information Enumerated by Intruders:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and DNS details
- Machine names
- Users and groups
- Applications and banners

Enumeration Techniques

Module 7

Enumeration Techniques

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

Enumeration Techniques

- 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)

Enumeration Techniques

- 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

NetBIOS Enumeration

Module 7

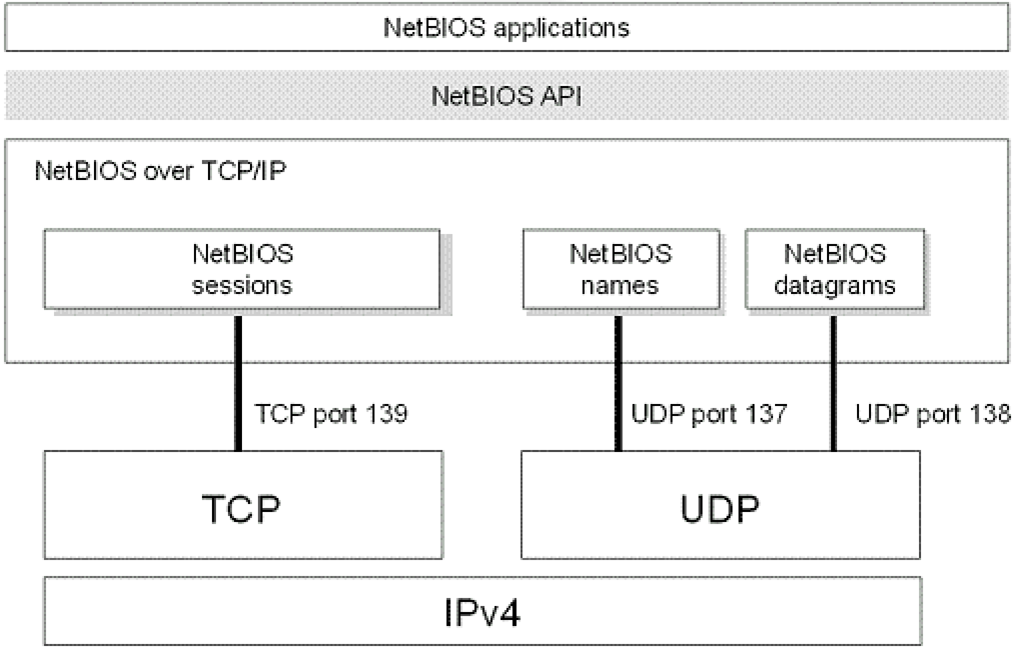
NetBIOS Enumeration

- 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 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 16th character is reserved for the service or name record type.

NetBIOS Enumeration

- Software applications on a NetBIOS network locate and identify each other via their NetBIOS names. (16 characters)
- Applications on other computers access NetBIOS names over UDP (NBNS)
- 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 "hang-up" command terminates a NetBIOS session.
- **NOTE**: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

NetBIOS Enumeration



NetBIOS Enumeration

- Attackers use the NetBIOS enumeration to obtain:
  - List of computers that belong to a domain
  - List of shares on the individual hosts in the network
  - Policies and passwords

NetBIOS Enumeration

- Attackers use the NetBIOS enumeration to perform:
  - Read/Write to a shared resource depending on availability of shares
  - Launch DOS on target
  - Enumerate password policies

NetBIOS Enumeration

- Nbtstat utility in Windows displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.
  - Run nbtstat command nbtstat.exe -c to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.
  - Run nbtstat command nbtstat.exe -a <IP address of the remote machine> to get the NetBIOS name table of a remote computer.

SNMP Enumeration

Module 7

SNMP Enumeration

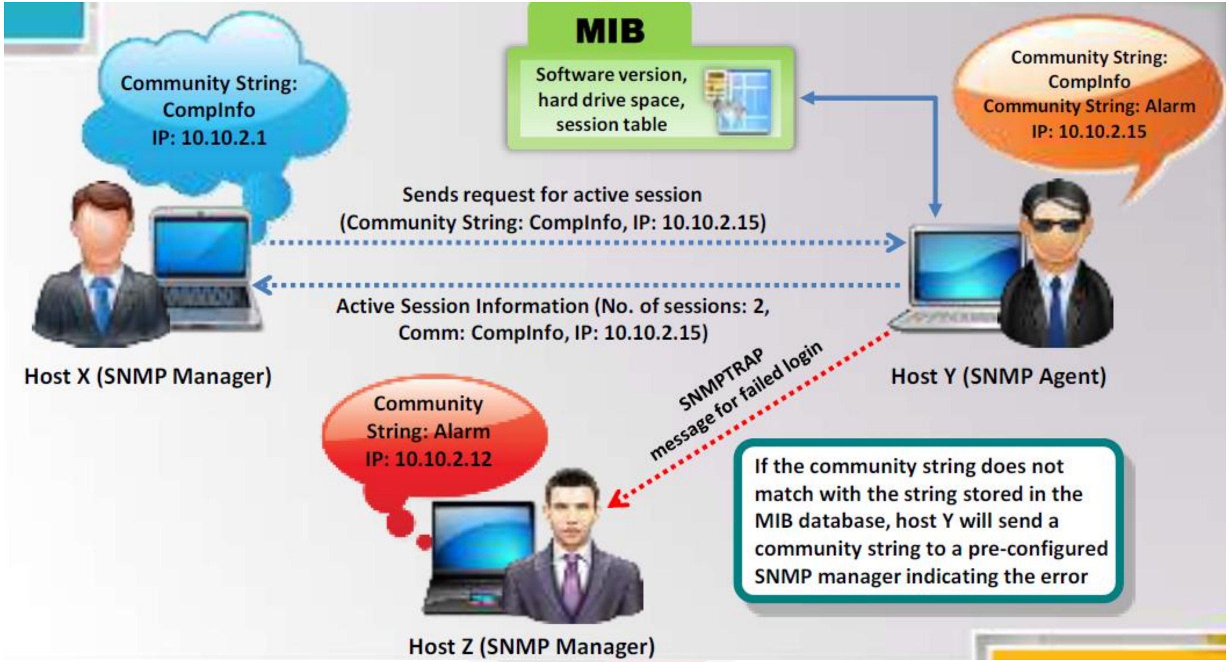
- SNMP (Simple Network Management Protocol) is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs and switches and other network devices on an IP network.
- SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.
- SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer.

SNMP Enumeration

Components of SNMP:

- **Managed Device:** A managed device is a device or a host (technically known as a node) 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 a managed device. Its primary job is to convert the information into SNMP compatible format for the smooth management of the network using SNMP protocol.
- **Network Management System (NMS):** These are the software systems that are used for monitoring of the network devices.

SNMP Enumeration


MIB
Software version, hard drive space, session table
Community String: CompInfo
IP: 10.10.2.1
Community String: CompInfo
Community String: Alarm
IP: 10.10.2.15
Sends request for active session
(Community String: CompInfo, IP: 10.10.2.15)
Active Session Information (No. of sessions: 2, Comm: CompInfo, IP: 10.10.2.15)
Host X (SNMP Manager)
Host Y (SNMP Agent)
SNMPTRAP message for failed login
Community String: Alarm
IP: 10.10.2.12
Host Z (SNMP Manager)

If the community string does not match with the string stored in the MIB database, host Y will send a community string to a pre-configured SNMP manager indicating the error

SNMP Enumeration

- SNMP holds two passwords to access and configure the SNMP agent from the management station:
  - **Read community string**: It is public by default; allows viewing of device/system configuration.
  - **Read/write community string**: It is private by default; allows remote editing of configuration.
- Attacker uses these default community strings to extract information about a device and to extract information about network resources such as hosts, routers, devices, shares, etc. and ARP tables, routing tables, traffic, etc.

SNMP Enumeration

Management Information Base (MIB)

- MIB is a virtual database containing 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 Identifiers (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.

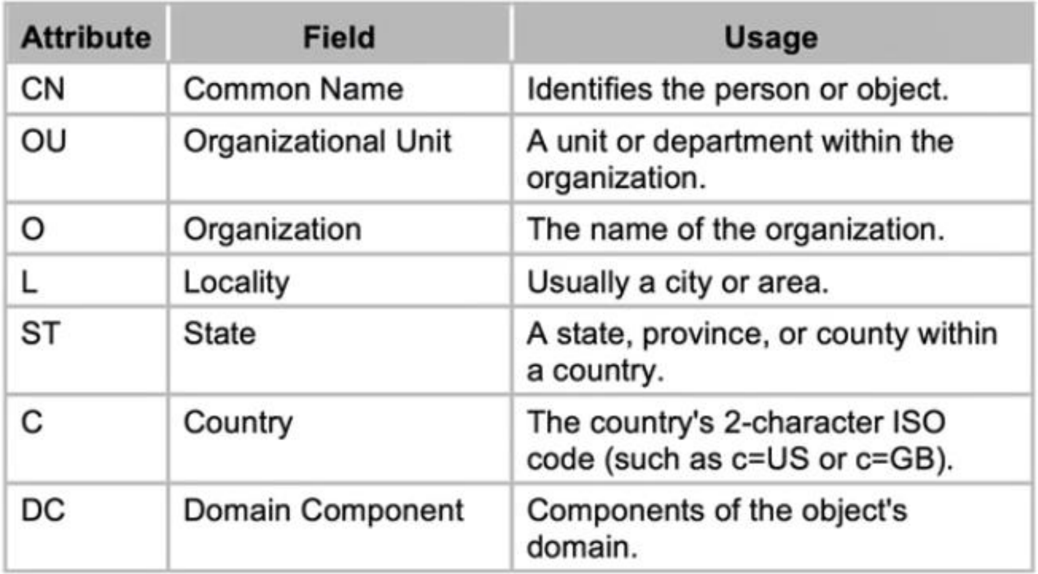
LDAP Enumeration

Module 7

LDAP Enumeration

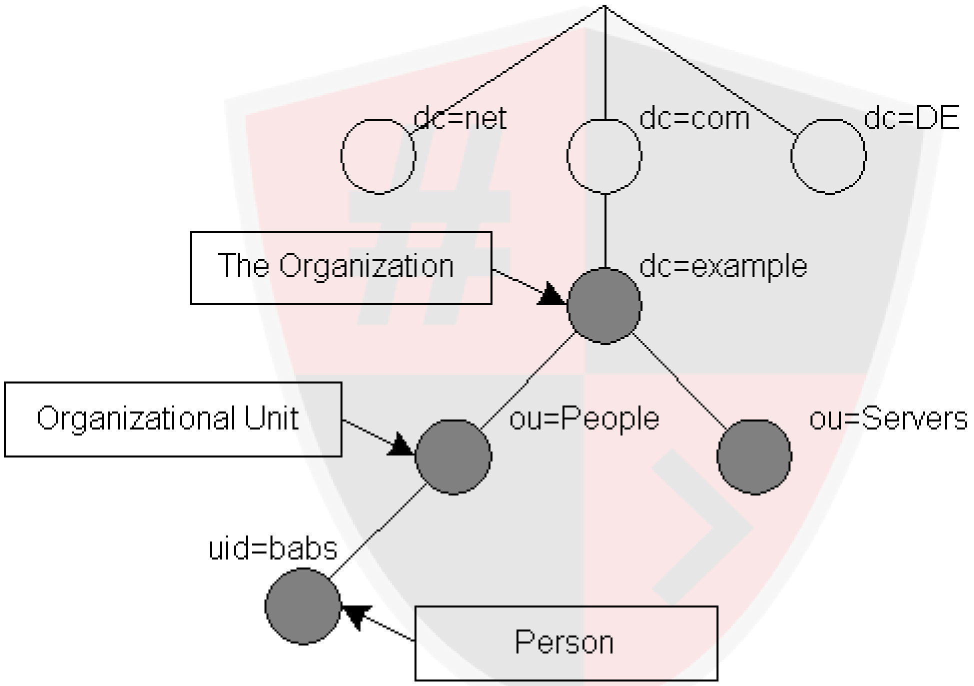
- Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services.
- Is a Hierarchical Compilation used to access directory listings within Active Directory or from other Directory Services.
- A client starts an LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 and sends an operation request to the DSA.
- Information is transmitted between the client and the 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.

LDAP Enumeration



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.

LDAP Enumeration



NTP Enumeration

Module 7

NTP Enumeration

- Network Time Protocol (NTP) 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 milliseconds (1/100 seconds) over the public Internet.
- It can achieve accuracies of 200 microseconds 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 if NTP server is in the DMZ

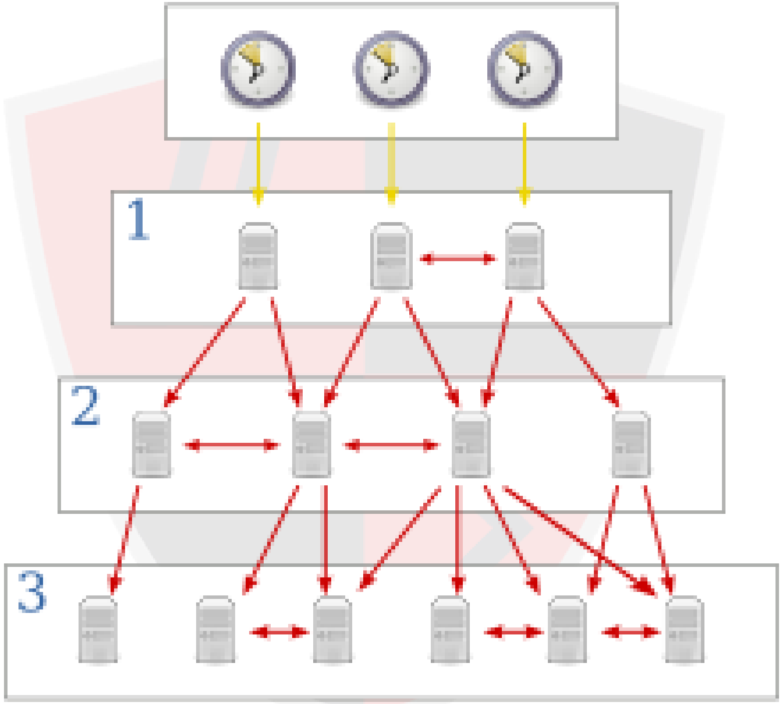
NTP Enumeration

Stratum 0

Stratum 1

Stratum 2

Stratum 3



SMTP Enumeration

Module 7

SMTP Enumeration

- Simple Mail Transfer Protocol is used to send emails to local or remote mail servers
- SMTP provides 3 built-in-commands:
  - **VRFY**: Validates users
  - **EXPN**: Tells the actual delivery addresses of aliases and mailing lists
  - **RCPT** TO: Defines the recipients of the message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can determine valid users on SMTP server.
- Attackers can directly interact with SMTP via the telnet prompt and collect list of valid users on the SMTP server.

DNS Enumeration

Module 7

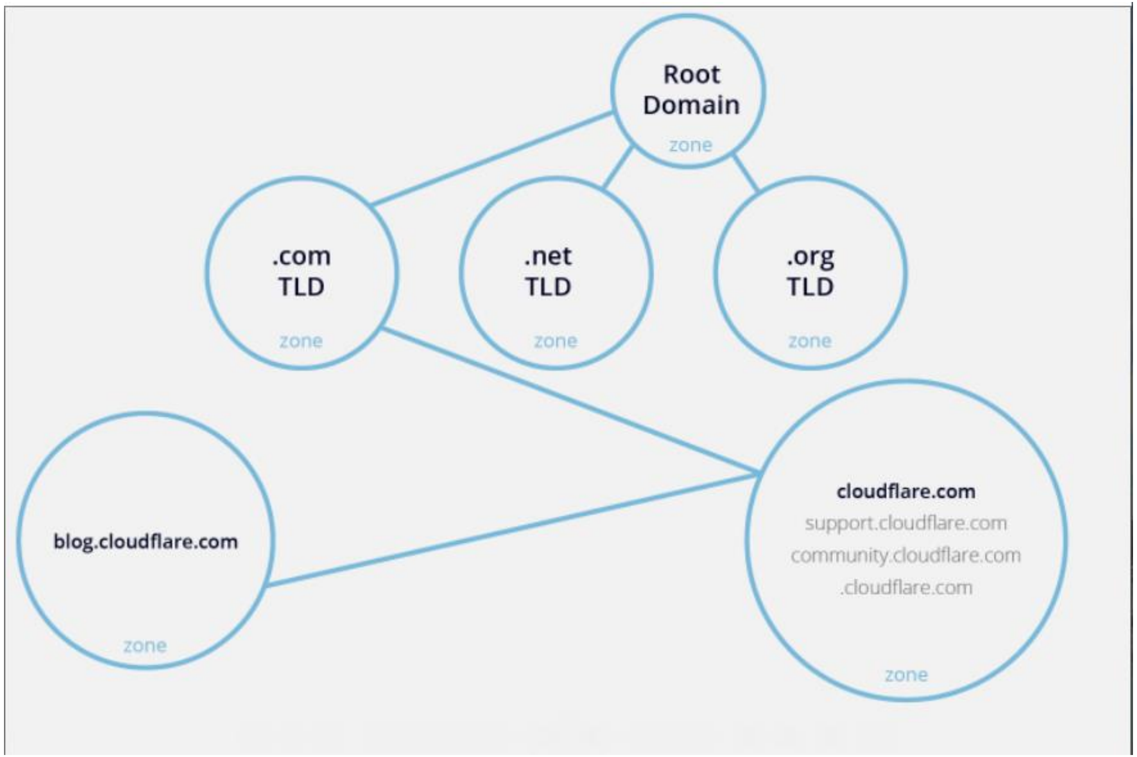
DNS Enumeration (Zone Transfer)

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

DNS Enumeration (Zone Transfer)

- A **DNS zone** is a portion of the DNS namespace that is managed by a specific organization or administrator.
- A DNS zone is an administrative space which allows for more granular control of DNS components, such as authoritative name servers.
- In fact, a DNS zone can contain multiple subdomains and multiple zones can exist on the same server.
- DNS zones are not necessarily physically separated from one another, zones are strictly used for delegating control.

DNS Enumeration (Zone Transfer)



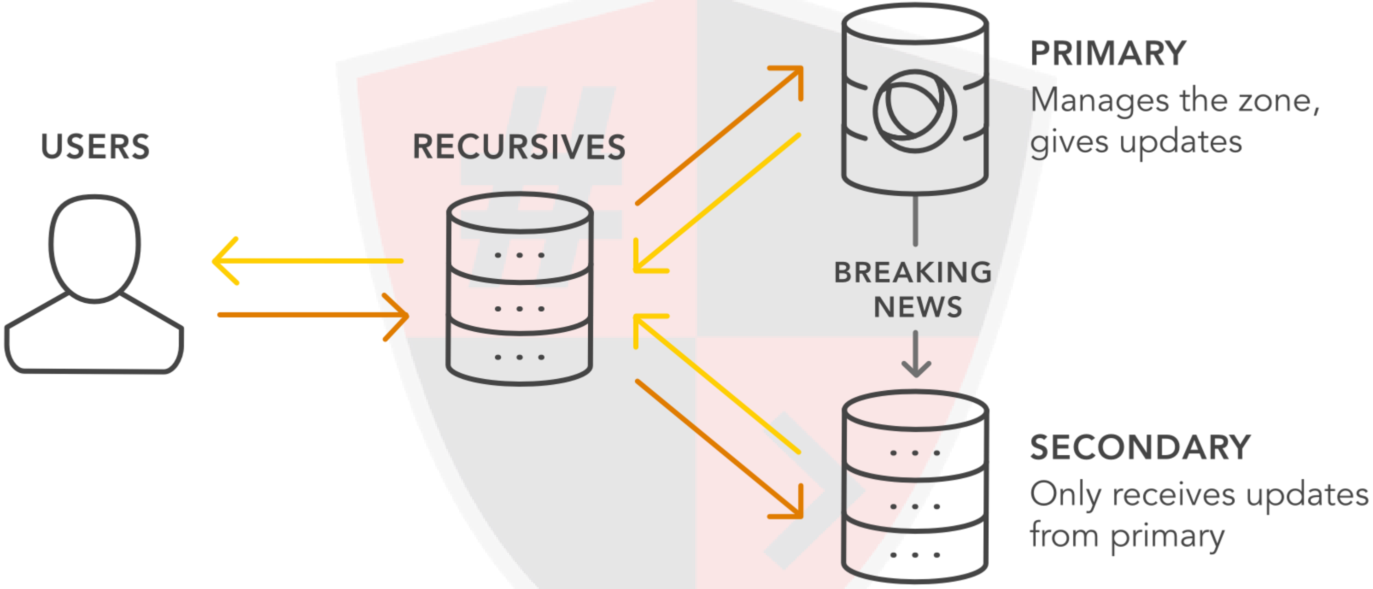
DNS Enumeration (Zone Transfer)

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

DNS Enumeration (Zone Transfer)

- A primary DNS server only has the master copy of the zone, and the secondary DNS will have a copy of the 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 called **Zone Transfer**.
- A zone transfer uses the Transmission Control Protocol (TCP) for transport, and takes the form of a client–server transaction

DNS Enumeration (Zone Transfer)



PRIMARY
Manages the zone, gives updates

SECONDARY
Only receives updates from primary

DNS Enumeration (Zone Transfer)

- 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.
- Zone transfers 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.

SMB Enumeration

Module 7

SMB Enumeration

- SMB stands for Server Message Block. It’s a protocol for sharing resources like files, printers, in general any resource which should be retrievable or made available by the server.
- It primarily runs on port 445 or port 139 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.
- The SMB protocol operates in Layer 7, and can be used over TCP/IP on port 445 for transport. Early dialects of the SMB protocol use the application programming interface (API) NetBIOS over TCP/IP

SMB Enumeration

- Important SMB implementations include: **CIFS, Samba, NQ, MoSMB, Tuxera SMB, Likewise**
- **SMB** uses 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 versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet.

Enumeration Countermeasures

Module 7

Enumeration Countermeasures

NetBIOS:

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

Enumeration Countermeasures

SNMP:

- Remove the SNMP 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 the access to null session pipes, null session shares, and IPSec filtering is restricted.

Enumeration Countermeasures

DNS:

- Disable the DNS zone transfers to the untrusted hosts
- Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
- Use premium DNS registration services that hide sensitive information such as HINFO from public
- Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks

Enumeration Countermeasures

- **SMTP:**
  - Configure SMTP servers to:
    - Ignore email messages to unknown recipients
    - Not include sensitive mail server and local host information in mail responses
    - Disable open relay feature

Enumeration Countermeasures

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
- Configure password policy
- Configure access control policy

Enumeration Countermeasures

- **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 the SMB protocol
  - Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

Enumeration Countermeasures

- **NTP:**
  - Configure MD5 layer
  - Configure NTP Authentication
  - Upgrade NTP version

HACKING

Is an art, practised through a creative mind.