**DAY-9**

Enumeration using FTP (File Transfer Protocol):

🡪Default usernames and passwords for FTP are ANONYMOUS/ANONYMOUS

Enumeration using shared resources:

🡪Network sharing in windows systems

Enumeration using NETBIOS:

🡪NETBIOS (Network Basic Input Output Systems)

1. List of machines within a domain

2. File sharing

3. Printer sharing

4. Usernames

5. Group information (User groups)

6. Password information (Password policy)

7. Services running

8. DNS information

🡪netbios is a service used in private network (LAN) to share data between devices running different applications

Tools like superscan and netbios enumerator can be used for netbios enumeration

In superscan

Go to windows enumeration

Options🡪 give username and password 🡪OK

IP/Hostname

Click enumerate

**GAINING ACCESS**

Gaining access is the fourth phase of ethical hacking

Access to a system can be gained by using different vulnerabilities in the following ways:

**1. Finding vulnerabilities manually with physical access**

This requires bypassing of the system to login

A beginner level password changing technique:

🡪Needs following privileges:

1. Physical access to the system

2. System should be booted up

3. User account should be logged in

Command line tool called **net user tools** to change the password

Cmd(admin)🡪net user (to find different users on system)

net user \_username\_ \_password\_

**2. Finding vulnerabilities using automated tools**

Automated tool nessus to find the vulnerabilities

Nessus installation:

🡪Download Nessus msi file

🡪Accept terms and install Nessus

After installation:

In default browser open

localhost:8834/welcomeToNessus-Install/welcome

click “connect via SSL”

select Nessus Essentials

Enter activation code

Create user account with username and password and remember them