# 4. Enumeration

## DNS Enumeration

### Practical 1: Using dnsenum tool from Kali Linux

Open a terminal window and enter a command in following syntax

dnsenum <target domain>

For example:

dnsenum virginia.edu
dnsenum wipro.com
dnsenum tata.com

### Practical 2: Using fierce tool from Kali Linux

Open a terminal window and enter a command in following syntax

fierce -dns <target domain>

For example:

fierce -dns wipro.com
fierce -dns virginia.edu

Apart from this there are several other tools available in Kali Linux that can be used for this purpose.
Some of them are dnsrecon, dig, nslookup etc.

### Practical 3: nbtscan command in Kali Linux

Open a terminal window and enter a command in following syntax

nbtscan <IP> or nbtscan <subnet>

For example:

nbtscan 192.168.0.100
nbtscan 192.168.0.0/24

## Practical 4: Enumeration using NMAP scripting

Using different scripts from NMAP can be used for enumeration purpose.

Syntax for using scripts in NMAP is like:

nmap –-script= <scriptname.nse> <target IP>

To simplify our work, open a terminal and enter following command

cd /usr/share/nmap/scripts/

ls | grep enum

Note: The above commands will show you all the scripts from NMAP with enum keyword. So you can try different scripts on your target.

For example:

nmap –-script=http-enum scanme.nmap.org

nmap –script=smb-enum-users 192.168.0.100

## Practical 5: Using enum4linux tool in Kali Linux

Open a terminal window and enter a command in following syntax

enum4linux <target ip>

For example:

enum4linux 192.168.0.100

enum4linux scanme.nmap.org