Hello Everyone! In this exercise, you will learn about DNSenum tool, an open-source tool for information gathering and how to use it.

Dnsenum is a multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous IP blocks. The main purpose of Dnsenum is to gather as much information as possible about a domain.

The following are the main functions of DNSenum Tool:

- Get the host's addresses
- Get the nameservers
- Get the MX record
- Perform axfr queries on nameservers and get BIND versions
- Get extra names and subdomains via google scraping
- Brute force subdomains from file, can also perform recursion on subdomain that have NS records
- Calculate C class domain network ranges and perform who is queries on them
- Perform reverse lookups on net ranges such as (C class or/and who is net ranges)
- Write to domain_ips.txt file IP-blocks.

What are we going to learn in this Exercise?

In this exercise, we are using DNSenum tool to gather DNS information of a domain and to discover non-contiguous IP blocks. For Step-by-Step process of using DNSenum tool follow the Lab Manual.

Thank You!!!