NET – 332

NETWORK SECURITY LAB

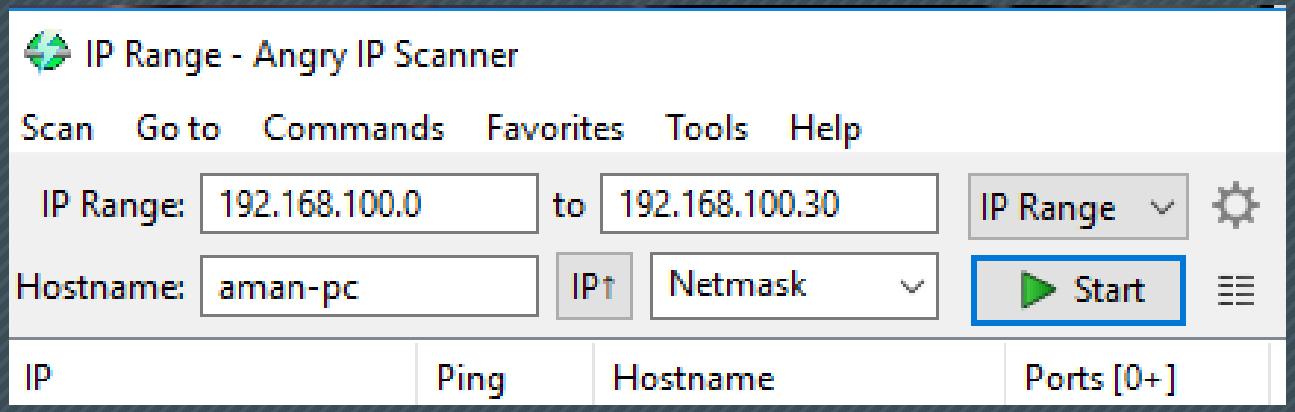
Lab 8. Detecting Active Systems and Enumerating Systems

Active Systems

- Active Systems are the live systems in any network that:
  - Have a IP address and are connected to intranet or internet
  - Have ports and services functioning to communicate with other resources on network
  - Have a user account configured to be accessed by the users of the network.

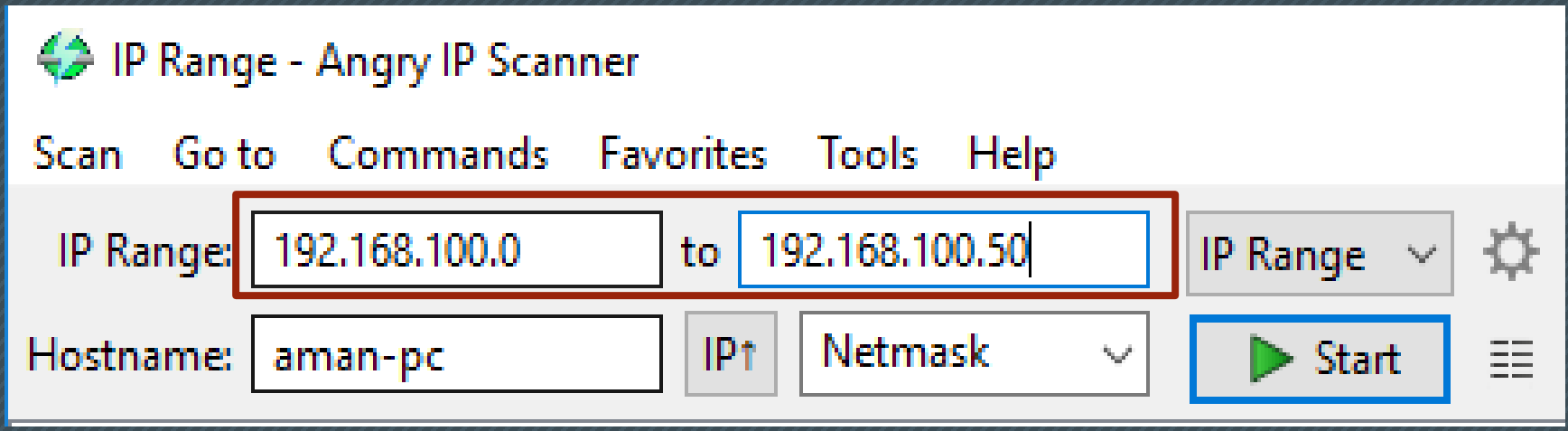
Hands on

- Download and install angry IP Scanner from Vdrive folder - Lab 8
  - Extract and Install the IP Scanner
  - Run the Angry IP

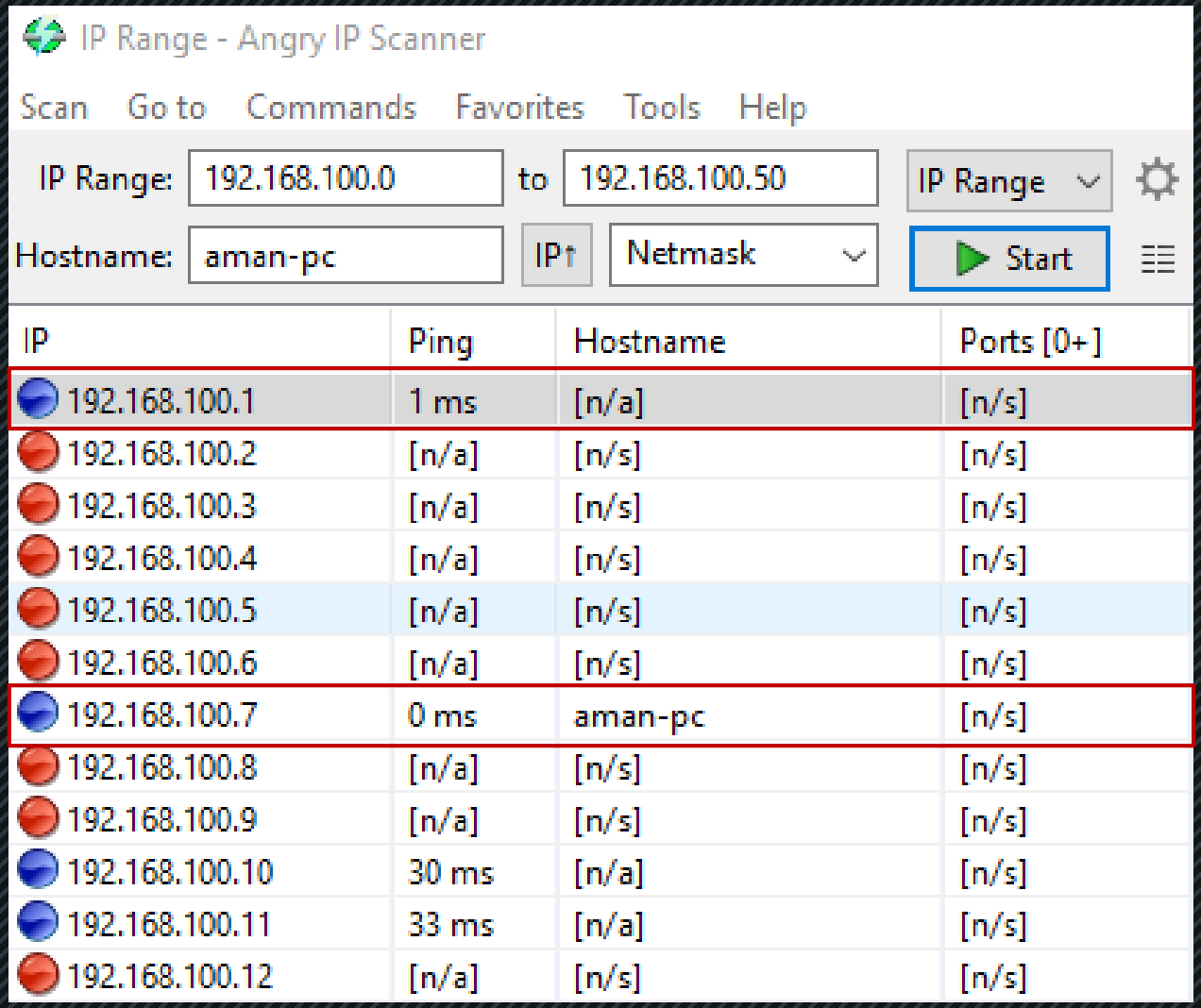


Scan Network - IP Range

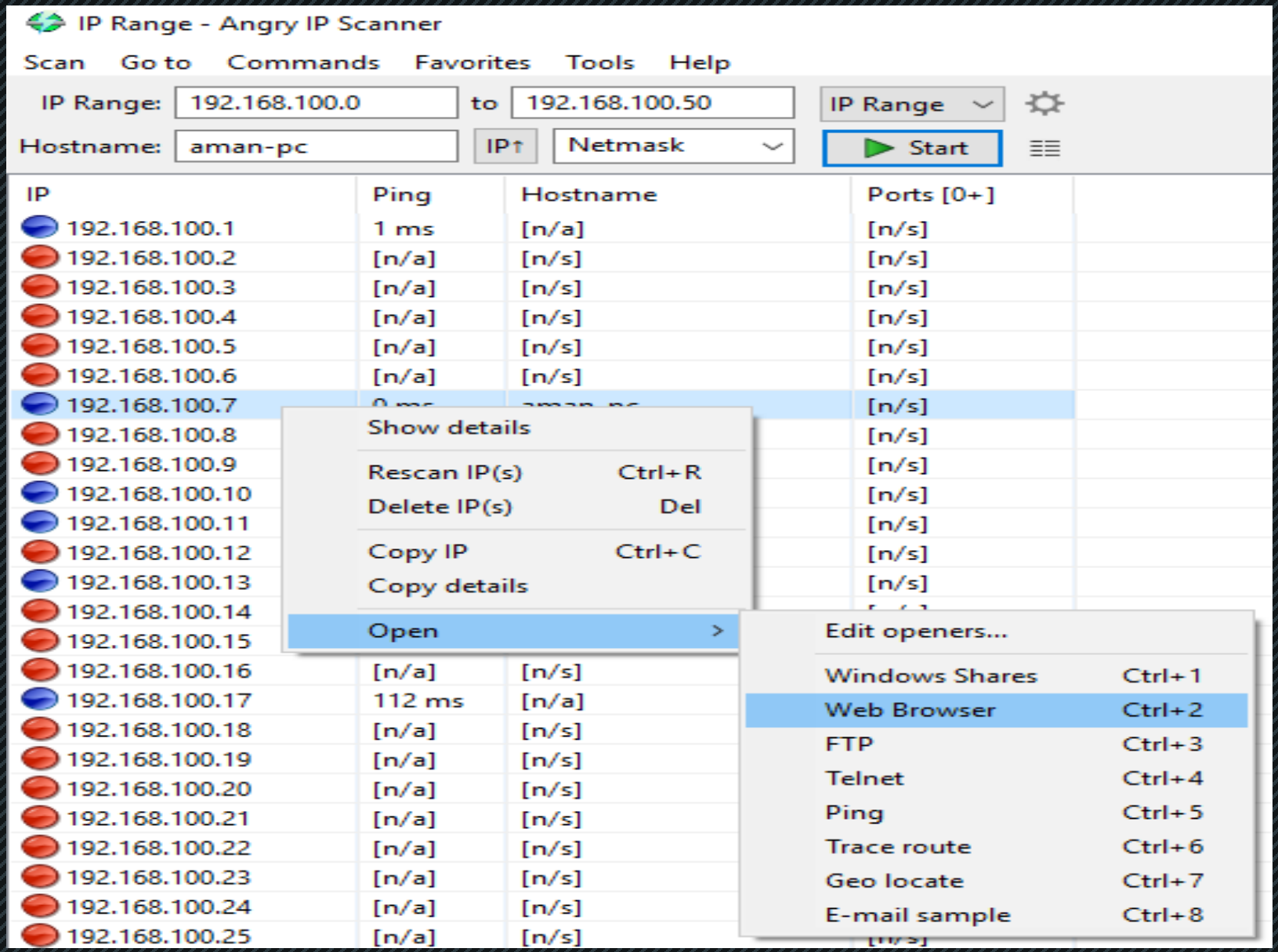
- In the IP Range enter a IP Range of 50 IP Addresses



Review Results



Deep Diving for Active Services



Analyzing Other Services

- Select any live system on the network (Marked Blue) and try the following:
  - Ping
  - Trace route
  - FTP
  - Web Browser
  - Windows Share

Enumerating Systems

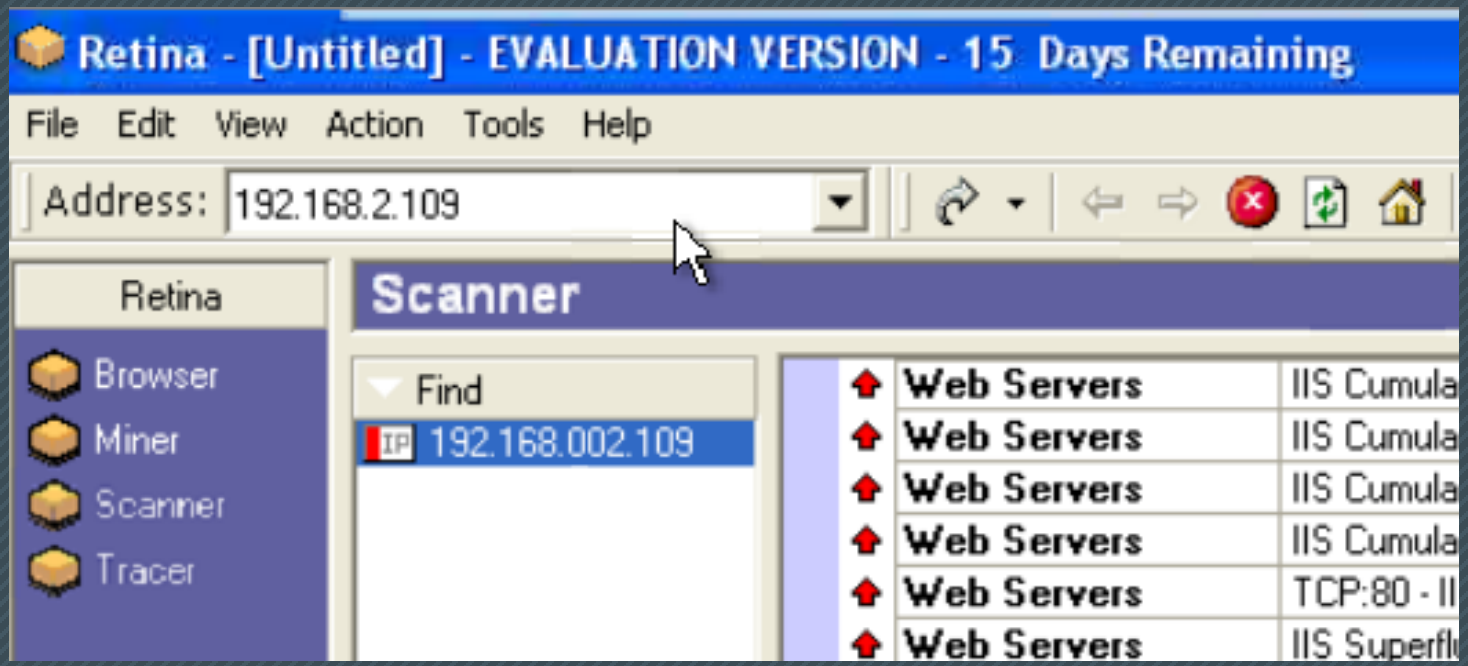
- Computer / Network enumerator is a program designed to scan the target and retrieve:
  - Usernames
  - Groups
  - Shares
  - Services

Basically, enumerators scan for vulnerabilities in the security of a target network

Identify Vulnerabilities that can be exploited

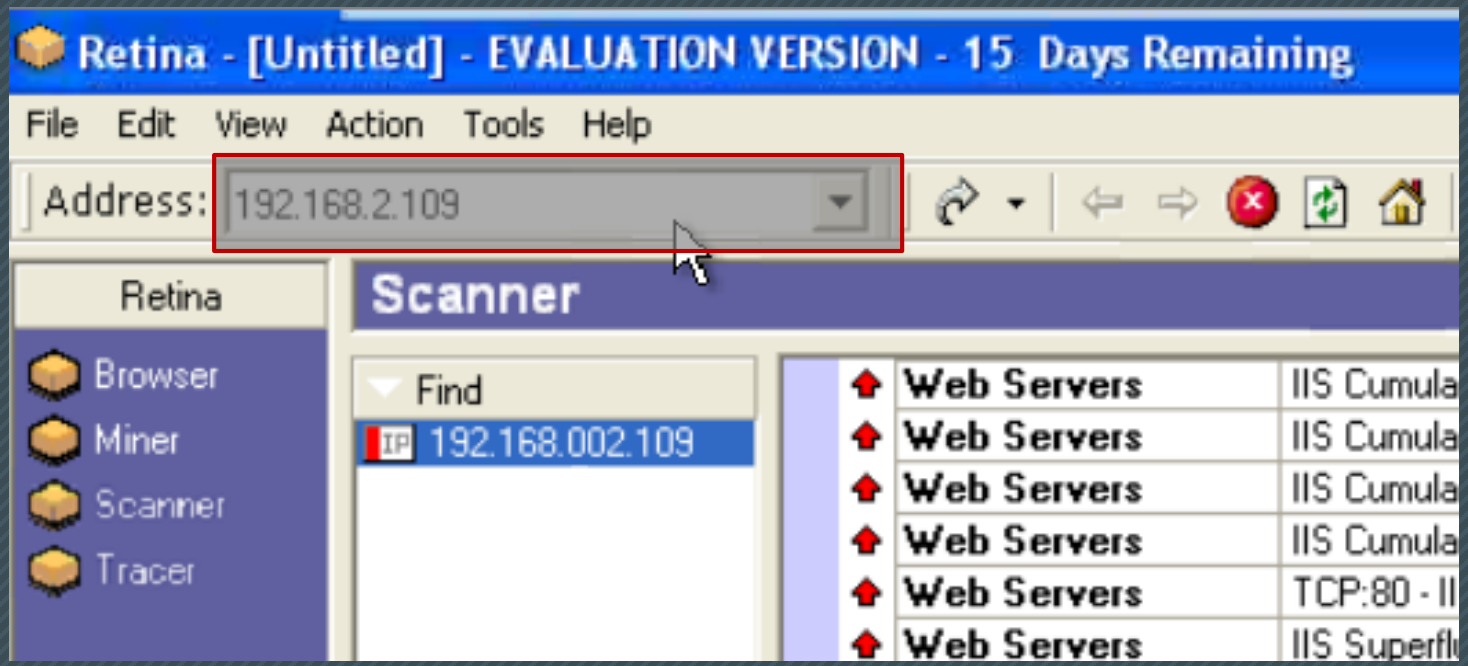
Enumerating Systems – Hands on

- Download and install Retina Scanner from Vdrive folder - Lab 8



Detailed Scanning using Retina

- Enter the target IP Address and click on Scan / Hit enter



Scanning Process

- The scanning using Retina might take a while as it performs an in-depth scanning of the target system/network.
- The scan will result in a detailed report containing:
  - Machine Hardware details
  - Operating System
  - Shares
  - Ports and Services

What is the use of information from Scanning and Enumeration

- The information collected through scanning and enumeration (passive) is used to:
  - Understand the technology of the target
  - Understand the security measures
  - Identify vulnerabilities
  - Decide on attack strategy by finalizing tools and resources to hack the target network.

Lab Activity - Handson

- Create a network of 3 computers in Oracle virtual box with:
- 2 virtual machines with different windows Operating systems
- 1 machine with Kali Linux
  - Use windows virtual machine (Scanner machine) 1 to install:
    - Angry IP Scanner
    - Retina Scanner

Lab Activity – Hands on … contd

- On virtual image 2 (windows – Victim Machine)
- Configure firewall to allow:
  - Remote desktop
  - TELNET
  - RPC
  - Sharing

Lab Activity – Hands on … contd

- Connect all the 3 virtual machines using internal network in Oracle virtual box (NAT)
- Scan the victim machine from the scanner machine using:
  - Angry IP Scanner
  - Retina Scan

Report Work:

- Prepare a report on the following:
  - Operating system details of victim machine
  - Shares available on victim machines
  - List of users on the victim machine
  - List of ports and services running on the victim machine.

Questions