



## Lab 8. Detecting Active Systems and Enumerating Systems

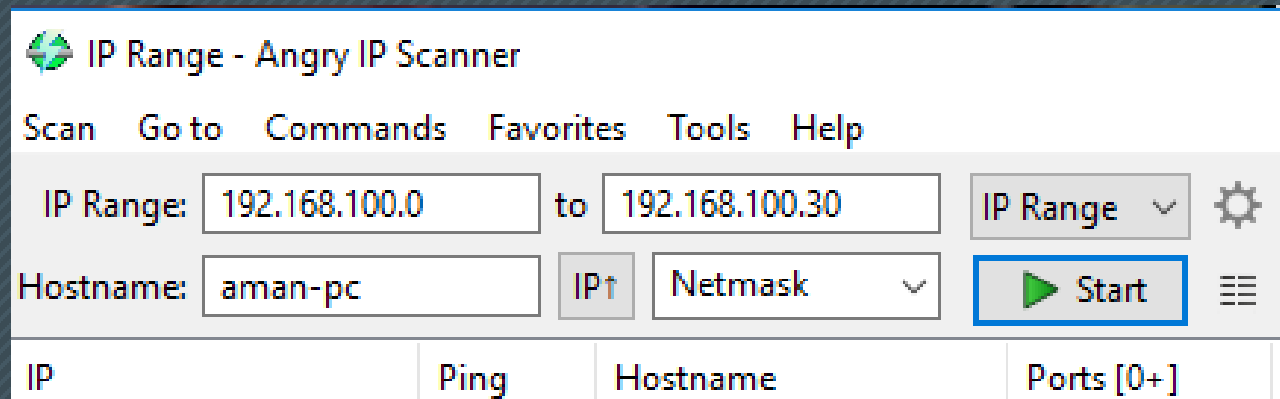
# Active Systems

– 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.

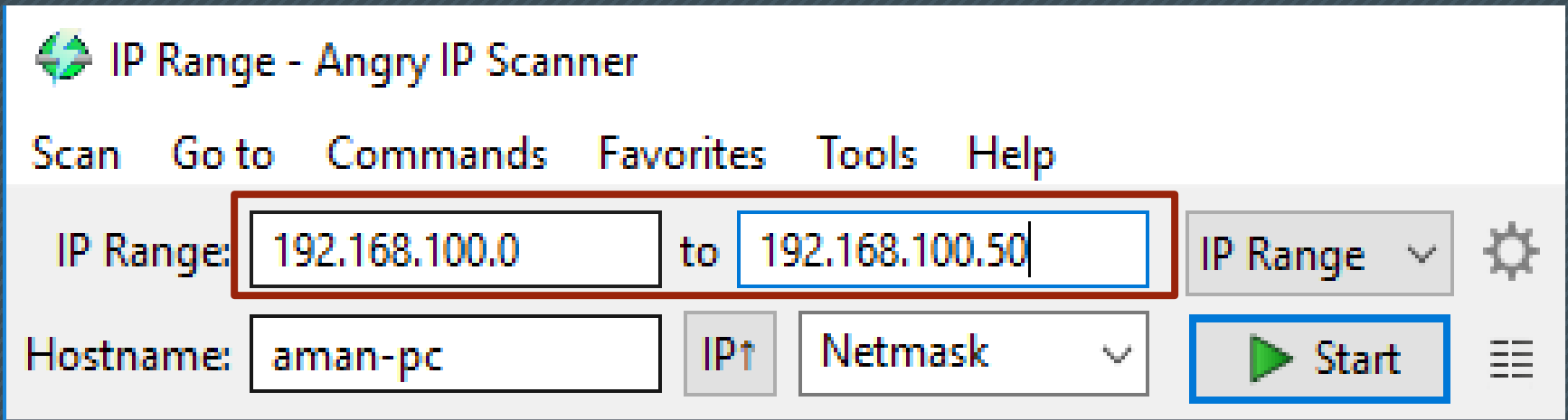
# Hands on

- 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



The screenshot shows the 'Angry IP Scanner' application window. The title bar reads 'IP Range - Angry IP Scanner'. The menu bar includes 'Scan', 'Go to', 'Commands', 'Favorites', 'Tools', and 'Help'. The main interface has two rows of input fields. The first row is for the 'IP Range', with the first field containing '192.168.100.0' and the second field containing '192.168.100.50', separated by the word 'to'. The second row is for the 'Hostname', with the field containing 'aman-pc'. To the right of the IP Range fields is a dropdown menu currently set to 'IP Range' with a gear icon. To the right of the Hostname field is a dropdown menu currently set to 'Netmask' with a gear icon. A green 'Start' button with a play icon is located to the right of the Hostname field. A red rectangle highlights the IP Range input fields, and a blue rectangle highlights the Start button.

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.100.0 to 192.168.100.50 IP Range

Hostname: aman-pc IP Netmask Start

# Review Results

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.100.0 to 192.168.100.50 IP Range

Hostname: aman-pc IP↑ Netmask

Start

IP	Ping	Hostname	Ports [0+]
192.168.100.1	1 ms	[n/a]	[n/s]
192.168.100.2	[n/a]	[n/s]	[n/s]
192.168.100.3	[n/a]	[n/s]	[n/s]
192.168.100.4	[n/a]	[n/s]	[n/s]
192.168.100.5	[n/a]	[n/s]	[n/s]
192.168.100.6	[n/a]	[n/s]	[n/s]
192.168.100.7	0 ms	aman-pc	[n/s]
192.168.100.8	[n/a]	[n/s]	[n/s]
192.168.100.9	[n/a]	[n/s]	[n/s]
192.168.100.10	30 ms	[n/a]	[n/s]
192.168.100.11	33 ms	[n/a]	[n/s]
192.168.100.12	[n/a]	[n/s]	[n/s]

# Deep Diving for Active Services

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.100.0 to 192.168.100.50 IP Range [v] [g]

Hostname: aman-pc IP↑ Netmask [v] [p] Start [g]

IP	Ping	Hostname	Ports [0+]
192.168.100.1	1 ms	[n/a]	[n/s]
192.168.100.2	[n/a]	[n/s]	[n/s]
192.168.100.3	[n/a]	[n/s]	[n/s]
192.168.100.4	[n/a]	[n/s]	[n/s]
192.168.100.5	[n/a]	[n/s]	[n/s]
192.168.100.6	[n/a]	[n/s]	[n/s]
192.168.100.7	0 ms	aman-pc	[n/s]
192.168.100.8			[n/s]
192.168.100.9			[n/s]
192.168.100.10			[n/s]
192.168.100.11			[n/s]
192.168.100.12			[n/s]
192.168.100.13			[n/s]
192.168.100.14			[n/s]
192.168.100.15			[n/s]
192.168.100.16	[n/a]	[n/s]	[n/s]
192.168.100.17	112 ms	[n/a]	[n/s]
192.168.100.18	[n/a]	[n/s]	[n/s]
192.168.100.19	[n/a]	[n/s]	[n/s]
192.168.100.20	[n/a]	[n/s]	[n/s]
192.168.100.21	[n/a]	[n/s]	[n/s]
192.168.100.22	[n/a]	[n/s]	[n/s]
192.168.100.23	[n/a]	[n/s]	[n/s]
192.168.100.24	[n/a]	[n/s]	[n/s]
192.168.100.25	[n/a]	[n/s]	[n/s]

Show details

Rescan IP(s) Ctrl+R

Delete IP(s) Del

Copy IP Ctrl+C

Copy details

Open >

Edit openers...

Windows Shares Ctrl+1

Web Browser Ctrl+2

FTP Ctrl+3

Telnet Ctrl+4

Ping Ctrl+5

Trace route Ctrl+6

Geo locate Ctrl+7

E-mail sample Ctrl+8

# 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

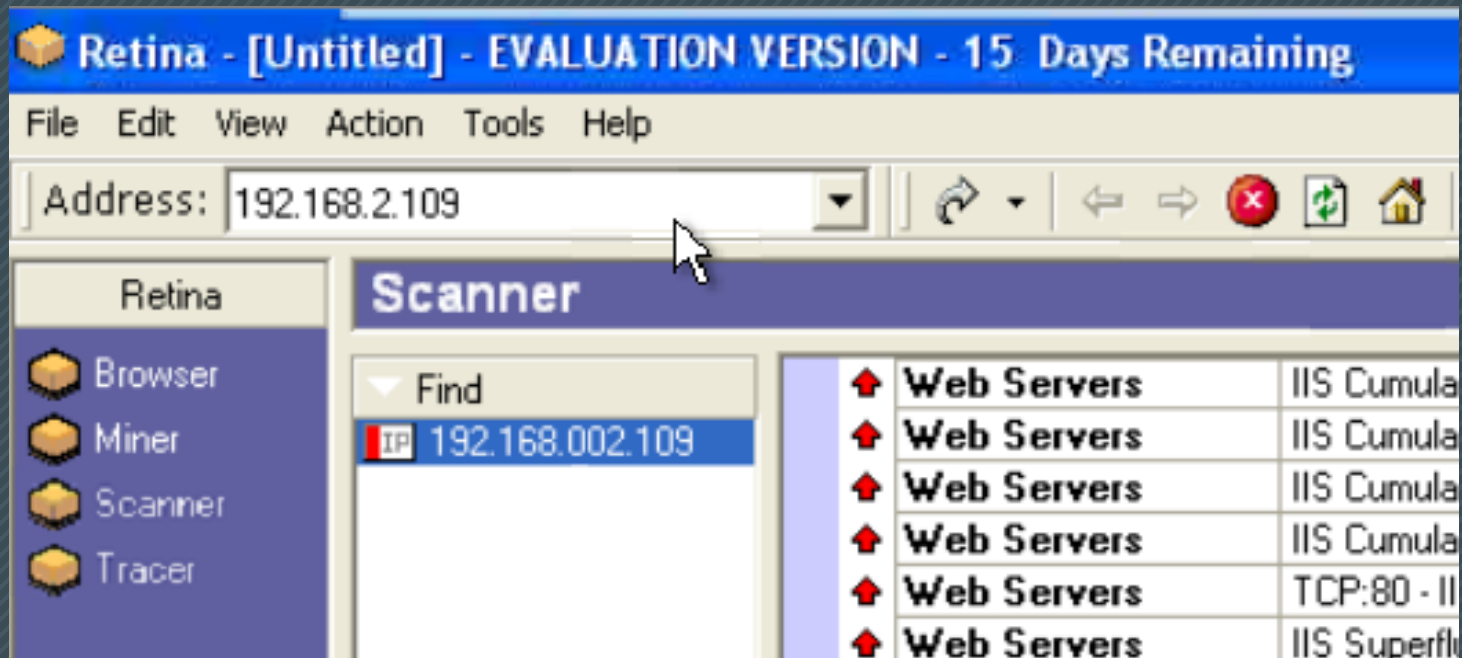
Basically, enumerators scan for vulnerabilities in the security of a target network

Identify Vulnerabilities that can be exploited



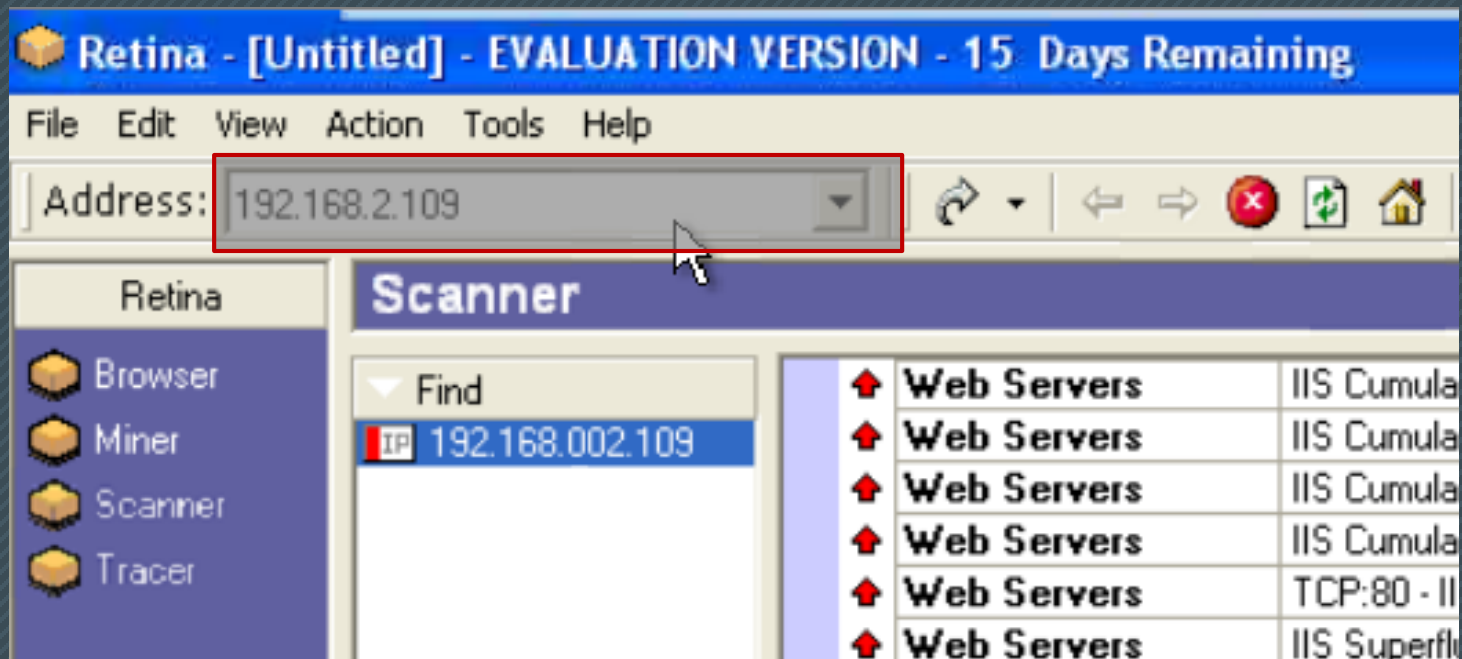
# Enumerating Systems – Hands on

- 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