**ASSIGNMENT 3**

**Introduction to Networking, Footprinting using reconnaissance enumeration**

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Basics of Networking | 2-6 |
| 2. | Footprinting in an reconnaissance enumeration | 7-8 |
|  |  |  |

# **Topic: Introduction to Networking, Footprinting in an Reconnaissance Enumeration**

ASSIGNMENT 3(DAY 3) Date:29-06-2022

1. **Topics of Networking**

**1.Networking Types**

* **Personal Area Network:**
* A PAN is a computer network for interconnecting electronic devices within an individual person’s workspace.
* It provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
* It is the smallest network which is very personal to the user and generally has a connectivity range up to 10 meters.
* **Local Area Network:**
* A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.
* A LAN is confined to a fairly small geographic area.  The clients and servers on a LAN are connected to the same channel, and are typically in the same building or in neighbouring buildings. Number of systems connected in LAN may vary from as least as two to as much as 16 million.
* LAN works under its own local domain and controlled centrally. Ethernet is most widely employed LAN technology and uses Star topology. LAN can be wired, wireless, or in both forms at once.
* **Metropolitan Area Network:**
* The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network.
* It can be in the form of Ethernet. It is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks.
* Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network.
* **Wide Area Network:**
* WAN covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. Since they are equipped with very high speed backbone, WANs use very expensive network equipment
* WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET).
* WAN maybe managed by multiple administration

**2.Networking Technologies**

* **Ethernet:**
* Ethernet is a widely deployed LAN technology. Ethernet shares media. It uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data.
* **Fast Ethernet:**
* To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet.
* It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100MBPS.
* **Giga Ethernet:**
* Giga-Ethernet provides speed up to 1000 MBPS.
* **VLAN:**
* Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains.
* Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN.
* **Internetwork:**
* A network of networks is called an internetwork, or simply the internet.
* It is the largest network in existence on this planet.
* Internet uses very high speed backbone of fiber optics.
* To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

**3.Networking Topologies:**

A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

* **Point-to-Point:**
* It contains exactly two hosts such as computer, switches, routers, or servers connected back to back using a single piece of cable.
* **Bus Topology:**
* All devices share single communication line or cable. It may have problem while multiple hosts sending data at the same time.
* Therefore, it either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
* **Star Topology:**
* All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection.
* That is, there exists a point to point connection between hosts and hub.
* **Ring Topology:**
* Each host machine connects to exactly two other machines, creating a circular network structure.
* To connect one more host in the existing structure, the administrator may need only one more extra cable.
* **Mesh Topology:**
* Here a host is connected to one or multiple hosts.
* This topology has hosts in point-to-point connection with every other host (Full Mesh) or may also have hosts which are in point-to-point connection with few hosts only.
* **Hybrid Topology:**
* A network structure whose design contains more than one topology is said to be hybrid topology.
* Internet is the best example of largest Hybrid topology.
* **Hierarchical Topology:**
* This topology imitates as extended Star topology and inherits properties of Bus topology.
* This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices.

**4.OSI MODEL:**

* The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols.
* the OSI provides a standard for different computer systems to be able to communicate with each other.
* The OSI Model can be seen as a universal language for computer networking. It’s based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.
* The OSI Model has the following layers:
* **Layer 1 – Physical layer:**
* This layer includes the physical equipment involved in the data transfer, such as the cables and switches.
* This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s.
* The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.
* **Transmission Media:**
* A transmission medium is a route that transmits information from a source to a receiver.
* Transmission mediums lie underneath the physical layer and the physical layer regulates them. Communication channels are another name for transmission medium
* Types are:
* **Twisted Pair Cable:**

This is the most widely used transmission medium cable. It consists of two distinct insulated conductor wires coiled around each other.

Several similar pairs are usually packed together in a protective sheath.

* **Coaxial Cable:**

It features an exterior plastic covering and two parallel conductors, each with its own insulated protective cover.

It operates in 2 ways: baseband and broadband.

* **Fiber Optics:**

It works on the principle of light reflection through a core composed of glass or plastic. The cladding surrounds the core, and the cladding is a less thick glass or plastic covering. It finds use in large-volume data transfer.

It is possible for the cable to be unidirectional or bidirectional.

* **Switching:**
* When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.
* It is a process to forward packets coming in from one port to a port leading towards the destination.
* Types of Switching are:
* **Circuit Switching:**

Circuit Switching is a dedicated path establishes between two communicating nodes before actual data transfer begins. The path means that connected sequence of physical links in which logical channel is dedicated to the connection.

Example: Telephonic Communication.

* **Packet Switching:**

Here the sender breaks the whole message into several packets of suitable length and consisting of sequential packet numbers.

No dedicated path establishes between the two end parties before data communication. The sender sends packets to the next node sequentially.

Each node after receiving a packet decides the next route for the packet, the routing decision done by a node in the path before sending every packet.

* **Layer 2 – Data Link Layer:**
* The Data Link Layer provides node-to-node data transfer (between two directly connected nodes), and also handles error correction from the physical layer.
* Two sublayers exist here as well--the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer.
* In the networking world, most switches operate at Layer 2. But it’s not that simple. Some switches also operate at Layer 3 in order to support virtual LANs that may span more than one switch subnet, which requires routing capabilities.
* **Functions of Data Link layer:**
* Framing –

Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver end, data link layer picks up signals from hardware and assembles them into frames.

* Error Control –

Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

* Addressing -

Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

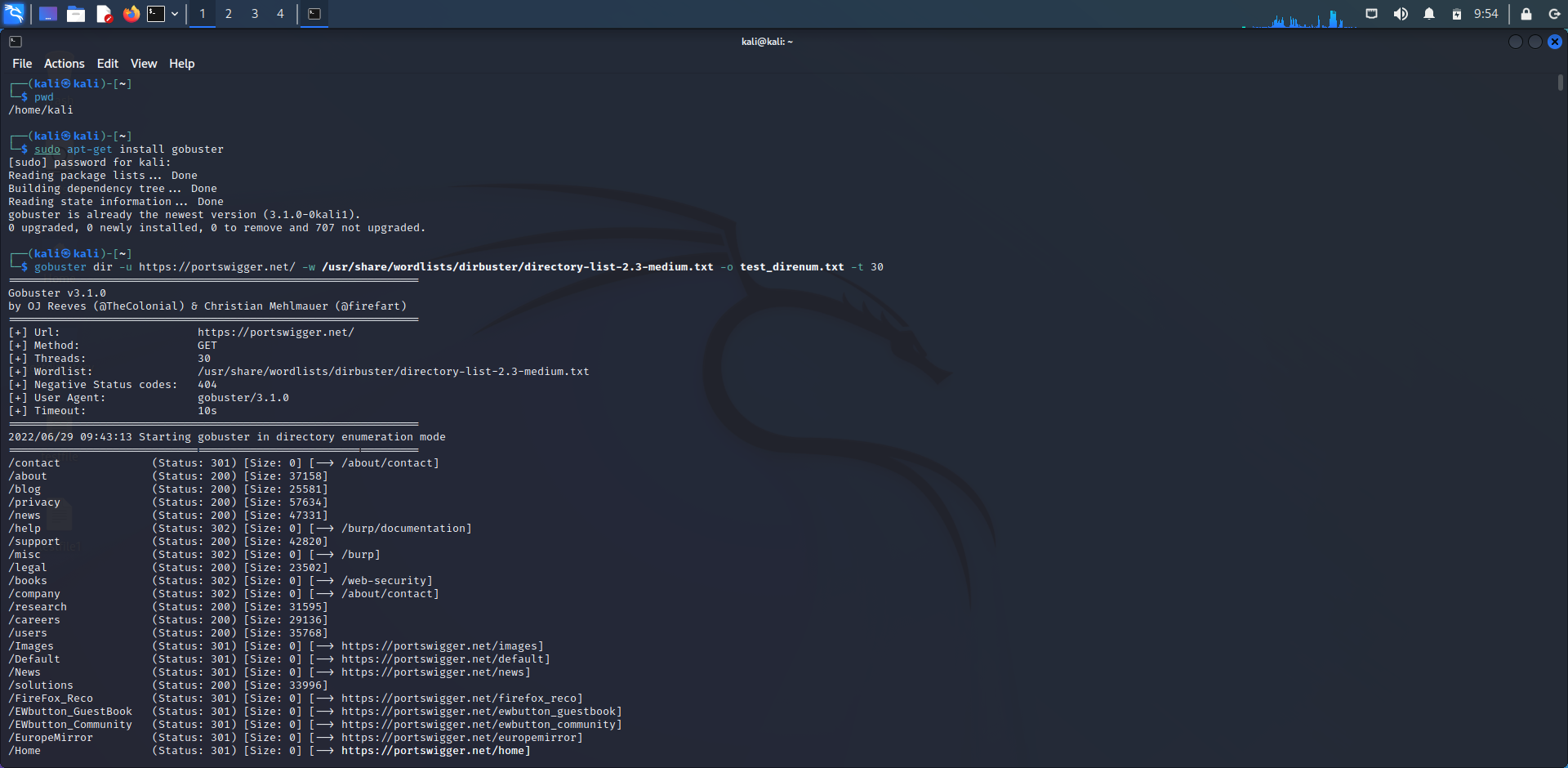
* Flow Control –

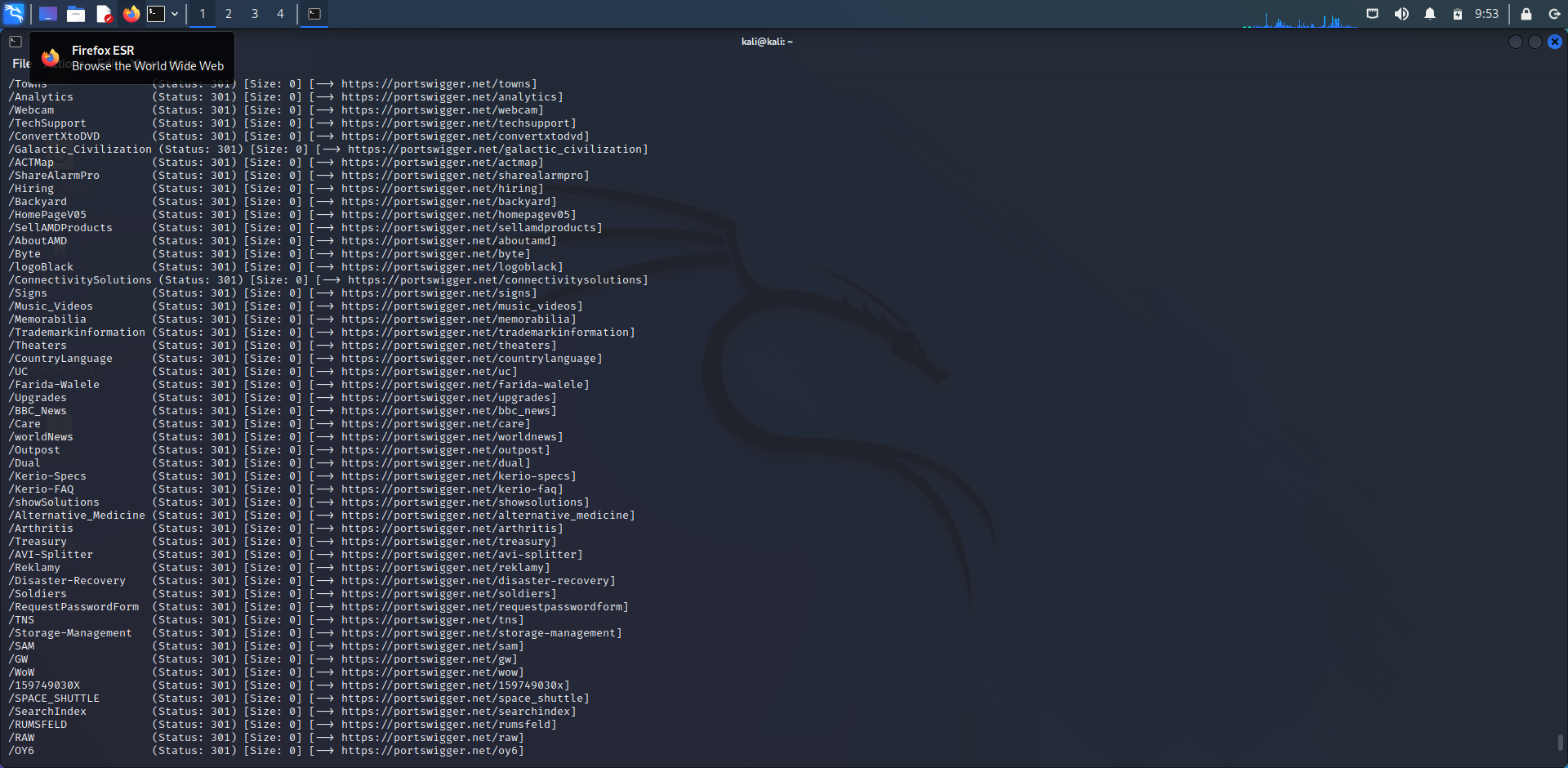
Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

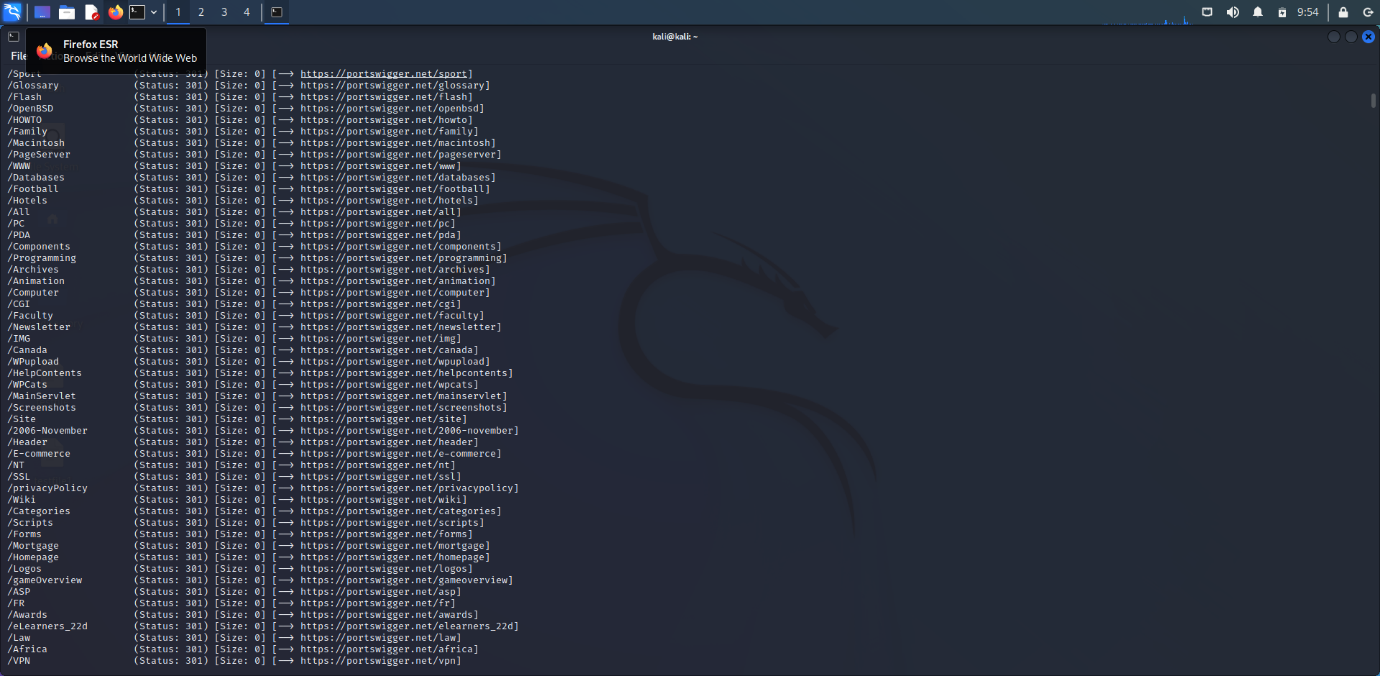
* **MAC Address:**
* Example of MAC address is 3C-95-09-9C-21-E1

having 6 octets, where the first three represent the OUI, the next three represent the NIC.

1. **Portswigger application result using dire num tool.**

****

****

****

**Name: I PRASANTI**

**Sic: 20BCEA56**

**Branch: CEN**