# CYBER SECURITY NETWORKING

Presented by
TAMILARASAN.M

The KaveryEngineering College

# CYBER SECURITY NETWORKING

# OUTLINE

1. NETWORKING BASICS
2. NETWORKING LAYER
3. NETWORKING TRANSPORT
4. FIREWALLS
5. WEB APPLICATION
6. CONCLUSION

# Networking basics

## Protocals And Networking

It is essential for Cyber Security Professionals to have a solid understanding of how computers communicate. There is much more happening behind the scenes of computer networks than what can be observed when using applications.

## The OSI Model

The OSI ("Open Systems Interconnection") model represents an easy and intuitive way to standardize the different parts required to communicate across networks.

The model makes it clear what is required to communicate on a network by splitting the requirements into multiple layers.

# Networking Layer

1. THE PHYSICAL LAYER
2. THE DATA LINK LAYER
3. THE NETWORKING LAYER
4. THE TRANSPORT LAYER
5. THE SESSION LAYER
6. THE PRESENTATION LAYER
7. THE APPLICATION LAYER

# Networking Transport

Computer systems often needs to talk to other systems; this is done by putting them on the same network. Several different technologies are in place to enable computers to talk over different kinds of networks. In this section we will go deeper into the protocols which are used in most networks.

The networks we are using consists of multiple protocols, some which are featured in this class. There are also many other protocols in use in networks, all which have the potential of having security risks associated with them.

# Firewalls

Firewalls are a central architectural element to any network. They are designed to keep out all network traffic, except traffic which we allow. Firewalls operate on Layer 4, typically controlling TCP and UDP access to internal assets. Next-Generation Firewalls operate on all the layers of the OSI model, including Layer 7.
Traffic entering a network, e.g. through a Firewall, is called ingress traffic. Traffic leaving is called egres s .

# Web Application

Web Applications are integral to almost everything we do, whether it is to access the Internet or to remotely control your lawnmower. In this introduction class we will cover the basics of web application security.

The Scheme is what defined the protocol to use. In our case it is the first part of the URL: https. When the scheme is not defined in the URL it allows the application to decide what to use. Schemes can include an entire array of protocols such as:

- HTTP
- HTTPS
- FTP
- SSH
- SMB

# Conclusion

The request header specifies what the client wants to perform on the target webserver.

It also has information regarding if it accepts compression, what kind of client is accessing and any cookies the server has told the client to present.