**# Course Content**

**Module 1 - Networking Concepts**

* What is Computer Networking?
* How does Networking Work?
* Types of Networks
* What is IP Address?
* IPv4 vs. IPv6
* Types of IP Address
* Role of Ports in Networking
* What is OSI Model and how does It Work?
* What is TCP/IP Model and How does It Work?
* OSI vs. TCP/IP Model
* What are Network Protocols?
* Types of Protocols
* How does TCP Work?
* TCP vs. UDP
* What is Domain Name?
* What is DNS?
* DNS Records and Their Uses
* What is Zone File?
* What is HTML Request?
* What is HTML Response?
* Types of Request Methods
* Capturing and Analyzing Network Packets (Wireshark)

**Module 2 – Introduction to Ethical Hacking**

* What is Ethical Hacking?
* Types of Hackers
* Types of Attacks on a System
* Cyber security Laws
* What is Linux?
* Cool Features of Linux
* Basic File System of Linux
* Basic Linux Commands
* Linux Commands (Practical)

**Module 3 – Setting up Ethical Hacking Lab**

* Installing Kali Linux in Virtual Box
* Configuring Kali Linux
* Installing Discover Tool
* Downloading a Good Wordlist
* Installing Burp Suite Pro
* Anonymous Configuration in Linux
* Configuring Proxy
* Configuring VPN
* Changing MAC Address
* Auto Run Shell Script (MAC Changer)
* Changing Wi-Fi MAC Address

**Module 4 – Footprinting and Reconnaissance**

* What are Footprinting and Reconnaissance?
* Types of Footprinting & Reconnaissance
* Use of Footprinting & Reconnaissance
* Footprinting Through Search Engines
* Footprinting using Advanced Google Hacking
* Techniques
* Footprinting Through Social Networking Sites
* Website Footprinting
* Email Footprinting
* DNS Footprinting
* WHOIS Footprinting
* NS Lookup
* Footprinting Through Discover Tool

**Module -1 Networking concept**

**What is computer networking?**

Computer networking is the communication between two or more computers with the use of different sources.

* Communication
* Sharing software
* Sharing file
* Sharing information
* Information preservation
* Security
* Sharing hardware
* Sharing data

ARP = Address Resolution Protocol, identify the devices connected to the internet.

**Types of networks in networking**

* LAN
* Wan
* Man

**What is LAN?**

A local area network is a collection of devices connected together in one physical location, such as a building, office, or home.

**What is MAN?**

= a metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or and given large are with multiple buildings. A man is larger than a local area network but smaller than a wide area network.

**What is WAN?**

= Wide area network is internet that connects computers within a wide geographical area. I.e. all over the world.

**What is IP address?**IP = Internet Protocol Address

Ipv4 address example

17.172.224.47 Information of country State ISP Device

|  |  |
| --- | --- |
| **IPv4** | **IPv6** |
| Address Size:  32-bit number | Address Size:  128-bit number |
| Address format:  Dotted Decimal Notation  192.159.252.76 | Hexadecimal Notation  3ffe:f200:0234:ab00:01  23:4567:8901:abcd |
| Prefix Notation:  192.149.0.0/24 | Prefix Notation:  3ffe:200:0234:/48 |
| Number of Addresses:  (2^32)4.7 billion addresses | Number of Addresses: (2^128)340 trillion, trillion,  Trillion addresses |

Types of IP Address

* Public
* Private
* Static
* Dynamic

Role of port in networking

* Total = 65535 ports
* States open closed filtered
* Well known 0 – 1023
* Registered 1024-49151
* Dynamic 49152-65535

**# Default ports**

|  |  |  |
| --- | --- | --- |
| Port Number | Protocol | Application |
| 20 | TCP | FTP Data |
| 21 | TCP | FTP control |
| 22 | TCP | SSH |
| 25 | TCP | SMTP |
| 53 | TCP, UDP | DNS |
| 80 | TCP | HTTP (WWW) |
| 110 | TCP | POP3 |
| 443 | TCP | SSL |

OSI vs. TCP / IP Model

What is OSI Model?

* Open Systems Interconnection model
* Defines functions
* 7 layers
* Standardize communication
* Bottom to Up

|  |
| --- |
| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Data layer |
| Physical |

How it works?

|  |
| --- |
| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Data layer |
| Physical |

Client Server

Data sharing is done with this process.

**Physical Layer**=Helps in bit streaming of the data that is being transferred. Hardware like router, Ethernet, etc. is included on this layer.

**Data Layer** = whatever errors are being generated, data layer will work on them.

**Network Layer** = this will find where is the data going smoothly or not through both wired and wireless medias without any misconfiguration and data breach. It works on source IP, address IP, source address & destination address.

**Transport Layer** = this layer will tell us whether this packet has been transported or not. Also known as link layer as it link software and hardware.

**Session Layer** = When two system connects a session is established. Those sessions should be connected, the session helps in that. Whether that network is connected or not, whether that session is active or not. If the session is not active, it will reconnect. Whether that session is authenticated or not, whether the authenticated person is connected to that session or not.

**Presentation Layer** = It performs the data manipulation. It will encode, encrypt convert to a zip file, and compress the data. Whatever process it is, it is done by the presentation layer.

**Application Layer** = this is our high level layer, It helps us to share resources.

This process, which is about data sharing, and accepting the data. The OSI layer is followed in between them. The data which is coming or going should work properly. The data that is being transferred should be proper, complete, securely transferred. So all this work is done by OSI model. Because of the OSI model, communication is happening in our networking has become easy.

**What is TCP / IP Model?**

* Transmission Control Protocol / Internet Protocol
* OSI Model Version
* 4/5 Layers
* Practical model
* Over WAN

|  |
| --- |
| Application Layer |
| Transport Layer |
| Internet Layer |
| Data-Link Layer |
| Physical Layer |

How it Works?

**TCP/IP 4-Layers Model TCP/IP 5-Layers Model**

|  |
| --- |
| Application Layer |
| Transport Layer |
| Internet Layer |
| Network Access Layer |

OSI vs. TCP/IP Model

TCP/IP OSI

|  |
| --- |
| Application  High-level API, Resource Sharing |
| Presentation  Data Formatting, Encoding, Encryption, Compression |
| Session  Authenticate, manage session and reconnections |
| Transport  Message segmentation, acknowledgment, reliable |
| Network  Multi node routing and addressing |
| Data Link  Flow and error control on physical link |
| Physical  Transmission of Physical bit Streams |

|  |
| --- |
| Application Layer |
| Transport Layer |
| Internet Layer |
| Network Access Layer |

Here, in both TCP/IP and OSI models, Application layer of TCP/IP combines Application, Presentation, and Session layers of OSI model.

Network Access Layer combines Data Link and Physical layers of OSI model.

By combining all these layers of OSI model, the TCP/IP model has been created, which practically used in Wide Area Network. This is only difference in the entire functioning of the OSI model in done by TCP/IP model.

Network Protocols and there working

What is Network Protocols?

* Set of rules
* How data is transmitted
* Device communication

When two devices communicate with each other, protocols are used. Protocol is the source that will carry data from one place to another. It will tell on which port the data will come or go. All the rules are followed by the protocols.

**Types of Protocols**

**TCP/IP – Internet Protocol Suite**

TCP/IP Model

|  |
| --- |
| Application |
| Transport |
| Internet |
| Network Access |

|  |
| --- |
| Telnet, SMTP, POP3, FTP, NTP, HTTP, SNMP, DNS, SSH, |
| TCP,UDP |
| IP, ICMP, ARP, DHCP |
| Ethernet, PPP, ADSL |

How TCP works?

|  |  |  |
| --- | --- | --- |
| URG (Urgent) | FIN (Finish) | RST (Reset) |
| Data contained in the packet should be processed immediately | There will be no further transmission | Resets a connection |
| PSH (Push) | ACK (Acknowledgement) | SYN (Synchronize) |
| Sends all buffered data immediately | Acknowledges the receipt of a packet | Initiates a connections between hosts |

Altogether there are 6 flags. Through whom TCP is helping the two devices communicate.

TCP vs. UDP

|  |  |
| --- | --- |
| TCP | UDP |
| TCP follows three way handshake | UDP (User Datagram Protocol) follows one way handshake. |
| In TCP, first the SYN packet goes, then SYN + ACK arrives, then an acknowledgement packet goes. Then a connection is established. | In UDP, a request comes, then just a response packet goes. Only one request is generated in UDP< after that the data transfer continues. |
| TCP works in wireless network. | UDP works in the wired network. |
| SYN  SYN ACK  ACK | Request  Response  Response |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Introduction of Domain name, DNS and Zone files**

What is Domain Name?

* Name of IP
* Easy to remember
* Examples: google.com, Facebook.com, etc.

What is DNS?

* Domain Name System/Server
* Address Book of Internet
* Translate Domain to IP
* Store all data in form of records in Zone file

Whatever relation or information is between a domain ad IP, it stores all that information in its own file, i.e. is called zone file. It saves all the information in the format of records. That is whatever the relation between the domain and the IP is, all that data will be stored in the zone file. All the information is collected and kept, hence it is called Address Book of Internet. So that if we go to any domain, he will ping us on the same IP.

Records in DNS & their use

|  |  |
| --- | --- |
| A | IP of domain name. |
| CNAME | Forwards domain and subdomain to another domain. |
| MX | Directs mail to email server |
| TXT | Any text by Admin. |
| NS | Name Server of DNS entry |
| SOA | Admin Info about a domain. |
| SRV | Specify port for specific service |
| PTR | Provides domain name in reverse-lookups. |

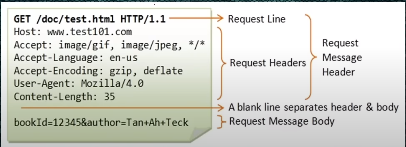
#What is zone file?

* A Text file of DNS
* Records of Domain
* IP Mapping
* Name Server. Zone

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#What is HTML request?

* A packet asking to load a website.
* Includes GET/POST, Headers and Body.



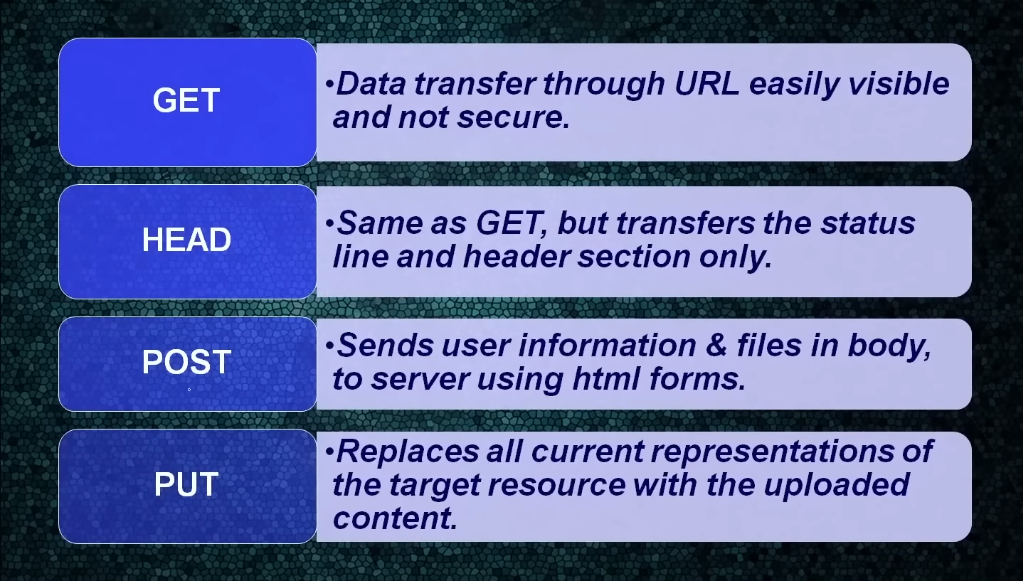
A sample of html request.

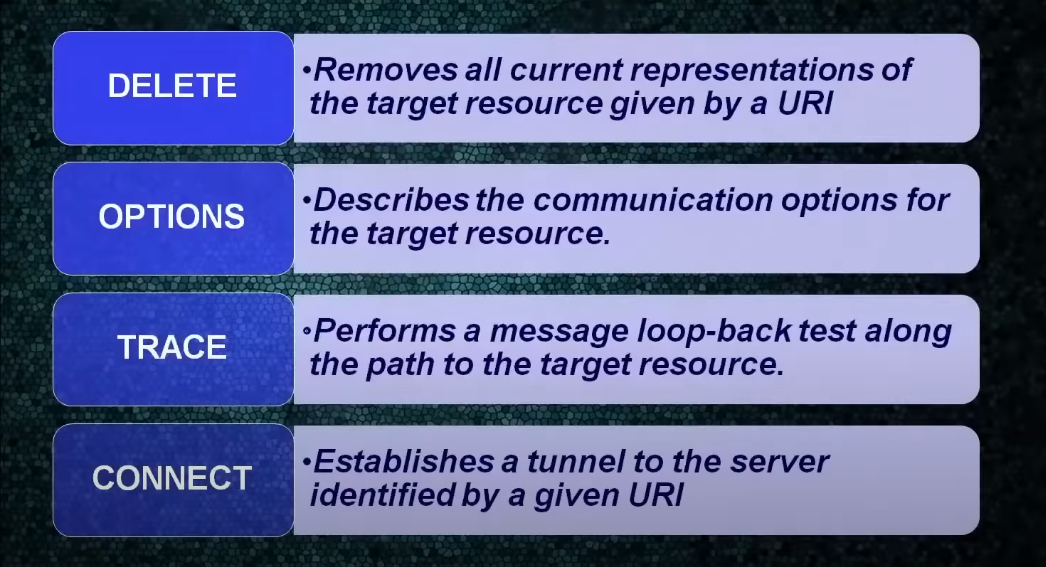
Here, the above request is sent by client to the server. Server accepts the request and give the response regarding the request so that client can access that. If there is no any error in your response then the website is opened properly.

#What is HTML response?

* Packet Providing Permission to access website and content.
* Includes GET.POST, Headers and Body.(complete program of that page)

#Types of Request Methods





**Module -2 Introduction to Ethical Hacking**

Types of hackers

1. White hat
2. Grey hat
3. Black hat

**Types of attack on a system**

1. Operating system attacks,

By using drawbacks of any operating systems getting authorization.

1. Misconfiguration attack,

Security misconfiguration vulnerabilities take place when an application component is vulnerable to attack as a result of insecure configuration option or misconfiguration.

1. Application level attack,

Gaining control of an application by attacking on vulnerabilities of the programmer of any web application

1. Shrink-wrap code attacks,

Attacking the devices, systems, applications whose vulnerabilities or patches are not yet released.

Cyber laws

1. The patents (Amendment) Act, 1999,
2. Trade marks Act, 1999
3. The copyright Act, 1957
4. Information Technology Act

What is Linux?

* Open source operating system
* Free to use
* Open source code to modify
* Based on Linux kernel
* First release on Sep-17-1991
* Developed by Linus Torvalds
* Made by Developers Community

Cool features of Linux

* Multiuser Capability
* Multitasking
* Portability
* Security
* Live CD/USB
* Graphical user interface
* Application support
* File system
* Open source

Basic file system of Linux

|  |  |
| --- | --- |
| /bin | Basic programs (ls, cd, mv, etc...) |
| /sbin | System Programs (fdisk, sysctl, mkfs etc...) |
| /etc | Configuration files |
| /temp | Temporary files |
| /usr/bin | Applications (apt, nmap, etc...) |
| /usr/share | Application support & data files |
| /home | Persona Directories of user’s. (/home/) |
| /root | Home Directory of super user(Admin) |

Basic Linux Commands

|  |  |
| --- | --- |
| help | Show you basic commands and there use. |
| man | Shows you complete manual of that command or program |
| ls | List all the folders and files of a directory. |
| cd | Change directory (one folder to another) |
| pwd | Print working directory. |
| dir | Same as ls |
| mkdir | Creates a directory (folder). |
| cp | Copy a file or folder. |
| mv | Move a file or folder |
| rm | Remove (delete) a file or folder |
| sudo su | Grant root privileges |
| cat | Show content of a file. |
| nano | Linux file editor. |
| pluma | File editor software |
| chmod | Change directory permission. |
| ./ | Executes shell file |
| bash | Execute shell programs. |
| apt-get update | Update packages list (URL’s) |
| apt-get upgrade | Update all installed software’s |
| apt-get install gedit | Install a particular software |

#Lab setup of Linux

\*Needs

1. Virtual Hardware
2. Can run Multiple OS
3. Easy configuration for time and resource saving
4. Safe Testing Environment

\*Requirements

1. Virtual box
2. VMWare workstation
3. ISO files
4. Virtual files