**What is Information Security**

**Information security**, sometimes shortened to **InfoSec**, is the practice of

preventing unauthorized access, disclosure, disruption, destruction,

modification, inspection, recording or destruction of information.

Information security's primary focus is the balanced protection of the

confidentiality, integrity, and availability of data and focuses on efficient policy

implementation, organization productivity.

**Elements of Information Security**

Information Security is a state of well-being of information and

infrastructure in which the possibility of theft, tampering, and disruption of

information and services are kept low or tolerable.

* Confidentiality
* Authenticity
* Integrity
* Non-Repudiation
* Authorization
* Availability

**The Security, Functionality and Usability Triangle**

The strength of these three components can define the level of Security in

any system.

**IP Tracing**

The IP address is one of the most critical pieces of information. To attack

the target computer, attackers need to identify the IP address of the target

computer. Attackers use different techniques to grab the IP address. Sending

tracking emails, or SMS, or some malicious links to grab the IP address of the

target computer is called as IP Tracing. In other words, extracting user details

(like location) based on IP address is known as IP Tracing or IP Lookup.

**IP Spoofing**

The basic protocol for sending data over the Internet network and many

other computer networks is the Internet Protocol (IP). The protocol specifies

that each IP packet must have a header which contains (among other things) the

IP address of the sender of the packet IP spoofing is the creation of Internet

Protocol (IP) packets which have a modified source address in order to either

hide the identity of the sender, to impersonate another computer system, or

both. It is a technique often used by hackers to invoke attacks against a target

device or the surrounding infrastructure.

IP address spoofing involving the use of a trusted IP address to overcome

network security measures, such as authentication based on IP addresses. It is

frequently used in denial-of-service attacks, where the objective is to flood the

target with an overwhelming volume of traffic, and the attacker does not care

about receiving responses to the attack packets.

**VPN**

A virtual private network (VPN) is allows you to create a secure

encrypted connection over a less secure network, such as the public internet to

another network. A VPN uses tunneling protocols to encrypt data at the sending

end and decrypt it at the receiving end. To provide additional security, the

originating and receiving network addresses are also encrypted. The encrypted

connection helps ensure that sensitive data is safely transmitted. It prevents

unauthorized people from eavesdropping on the traffic and allows the user to

conduct work remotely. A VPN is created by establishing a virtual point-topoint connection through the use of dedicated circuits or with tunneling

protocols over existing networks

**VPS**

A VPS is a server created using

software virtualization. It functions like a

physical server, but it is a virtualized instance

created within a server. A single physical

machine can host multiple virtual private

servers. A cloud-based VPS may be hosted

across multiple servers. A VPS runs its own

copy of an operating system (OS), and

customers may have superuser-level access to

that operating system instance, so they can

install almost any software that runs on that OS. The technology behind VPS

hosting is similar to that of VMware or Virtual Box. These programs allow you

to run several virtualized operating systems on one machine.

**Proxy**

A proxy server acts as a gateway between the device and the internet. It’s

an intermediary server separating end users from the websites they browse. A

proxy server thus functions on behalf of the client when requesting service,

potentially masking the true origin of the request to the resource server. Proxy

servers provide varying levels of functionality, security, and privacy depending

on company policy. If a person using a proxy server, internet traffic flows

through the proxy server on its way to the requested address. The request then

comes back through that same proxy server, and then the proxy server forwards

the data received from the website to the requested device. This serves as a

method to simplify or control the complexity of the request, or provide

additional benefits such as load balancing, privacy, or security.

**Requirements to run Parrot Security OS on the Host machine**

**Hardware:**

* Minimum 4/8 GB RAM
* AMD2016 Model / intel core i3/i5/i7 processor
* Minimum 80 GB Hard disk
* Minimum 15 Mbps internet speed

**Software**

* Virtual box software
* Parrot Security OS virtual machine image file (.ova)
* Metasploitable 2 virtual machine