# 1. Introduction to Network Security

Secure has its etymological roots in *se* without, or apart from, and *cura* to care for, or be concerned about. It might he said a computer system is secure if it is safe from threats, which now a days is feasible only if it lives in an isolation. That is why it is said that a truly secure computer is one that is not plugged into a network or any sort of electricity. In such a case the numbers of exploits are minimized, i.e. existing hidden weaknesses that can hit the system are reduced. But by doing so functionality of the system is severely minimized, which is undesired. It is need of the hour to have computer systems with varying functionalities. Also, these systems should not be placed under isolation, need is to have networked systems connected within a limited domain or sometimes even beyond that. Today, the world is converging into a global village and in the near future, organizations would be even more interconnected, having homogenous or heterogeneous setups. This global scenario leads to an increase in the vulnerabilities to which systems are exposed when connected to the network. Therefore, when there is compelling need to have global reach and maximum clientage, network security becomes utmost concern for the enterprises.

The security in computer networks is a rapidly growing area of concern [1]. Most of the valuable information resides on the network, making network an inevitable entity for survival. There is proliferation of the networks in daily lives, he it an academic or business environment. These small networks are connected further to wide area networks which in turn forms the basis of Internet. The Internet is the 'worlds largest collection of networks that reaches universities, government labs, commercial enterprises, and military installations in many countries" [2]. Although the Internet connects larger network such as those belonging to large communication companies. It consists primarily of local area networks (LANs) [3]. The principle method of communication on the Internet is the TCP/IP (Transport Control Protocol/Internet Protocol) protocol suite. The Internet, however, is increasingly becoming an environment with multiple protocols [4].

The basis for the Internet was an experiment begun in 1968 by the Defense Departments Information Processing Techniques Office (ARPA/IPTO) to connect computers over a network in order to ensure command and control communications in the event of a nuclear war. The original network was known as the ARPAnet, and the project quickly became a 'straight research project without a specific application' [5]. In the 1980s, the number of local area networks increased significantly and this stimulated rapid growth of interconnections to the ARPAnet and other networks. These networks and interconnections are known today as the Internet [6] .

## 1.1 Primary Network Stakeholders

Computers that communicate across the internet are known as a host computer, or simply host [3] . A host's connection to the internet can be continuous or part- time, it can he through dialup or direct connections [7]. Each host computer is identified by both a unique 32-bit if address (internet protocol address) and fqdn (fully qualified domain name). Each of these has two parts: one that specifies the host computer, and another that specifies the location (either physical or organizational) of the host computer [8]. Ip addresses are generally written as four decimal numbers, each between 0 and 255, and each representing an 8-hit octet of the address. These numbers are separated by dots and notation is called dotted decimal notation, e.g. 172.31.1.6 is a valid IP address. IP addresses are logical entries binded with respective physical address of the network interface card, more popularly called as MAC address. All the communications from one network node to another node happens via physical layer of ISO model, i.e. machine is recognized by the network through its MAC address.

In order to setup a TCP/IP network each machine should be unicue1y identifiable via its IP address. These IP addresses are further used in conjunction with subnet masks which draw a boundary between network and host portion of an IP address. There are two predominant methods currently used to divide the 32 bits of an IP address into the host and network portions [3]. The original addressing scheme was to use the first octet to identify the network and then to use the other three octets to identify the host. This limited the Internet to 256 networks. With the rapid growth in the number of LANs (Local area networks), this addressing scheme was abandoned in favor of an addressing scheme with three primary classes. This remains the most widely used addressing scheme [4]. In this "classical" addressing scheme, called classfull addressing, entire32 bit address space is divided as elaborated in Table 1.1.

**Table 1.1: Internet Network Classes**

| Class | Leftmost (Class) Bits | Number of Network Bits | Maximum Number of networks | Maximum Number of Hosts per Network |
|---|---|---|---|---|
| A | 0 | 7 | 127 | 16,777,216 |
| B | 10 | 14 | 16,384 | 65,536 |
| C | 110 | 21 | 2,097,152 | 256 |
| D (Multicast) | 1110 | N/A | N/A | N/A |
| E (Reserved for future use) | 1111 | N/A | N/A | N/A |

A newer internet addressing scheme, the classless inter domain routing (CIDR) method, is also being used these days extensively. Using CIDR, the most significant k bits of each address specifies the network, and the remaining (32 - k) bits specify the host. The size of k is unrestricted [3], e.g. 172.31.1.6/24 is CIDR representation of 172.31.1.6 with 255.255.255.0 subnet. Domain is a "name associated with an organization, or part of an organization, to help identify systems uniquely [9] ." Domain names are assigned because users find it easier to work with symbolic names rather than IP addresses [4]. FQDN like www.tiet.edu gets translated into IP address via DNS (Domain Name System) and finally into MAC address via ARP (Address Resolution Protocol). Each host computers domain name is a group of labels (words or letters) separated by clots. Similar to IP addresses, domain names are divided into a host portion and a location portion. The leftmost label or group of labels identifies the host [9], and the rest usually refer to the location. An example is www.tiet.edu, which is a fully qualified domain name, because it has complete host and domain portions.

In an Internet address such as tiet.edu the .edu part is known as a Top Level Domain, or TLD. So-called "TLD registry" houses online databases that contain information about the domain names in that TLD. The .edu registry database, for example, contains the Internet whereabouts or IP address of tiet.edu. At the heart of the DNS are thirteen special computers,

called root servers. They are coordinated by Internet Corporation for Assigned Names and Numbers (ICANN) and are distributed around the world. All thirteen contain the same vital information regarding domains.

ICANN is responsible for managing and coordinating the Domain Name Services to ensure universal resolvability. ICANN is a global, non-profit, private-sector coordinating body acting in the public interest. ICANN ensures that the DNS continues to function effectively by overseeing the distribution of unique numeric IP addresses and domain names. It also oversees the processes and systems that ensure that each domain name maps to the correct IP address.

### 1.1.1 World Internet Usage

Lotto has estimated the growth in the number of hosts and domains on the Internet since 1981. Since 1986, estimates were made using the ZONE (Zealot of Name Edification) program [10]. In July 1996, the Internet connected together a minimum of approximately thirteen million host computers. The survey counted the number of domain names that had IP addresses assigned to them. However, by July 1997, the Domain Survey was not able to count a significant portion of the hosts in the domain system, due to some organizations restricting download access to their domain data. The blocking of downloads (or zone transfers as they are called) had increased to the point where in the July 1997 survey it could only download 75% of the domains. A new survey technique was proposed: it counts the number of IP addresses that have been assigned a. name [11].

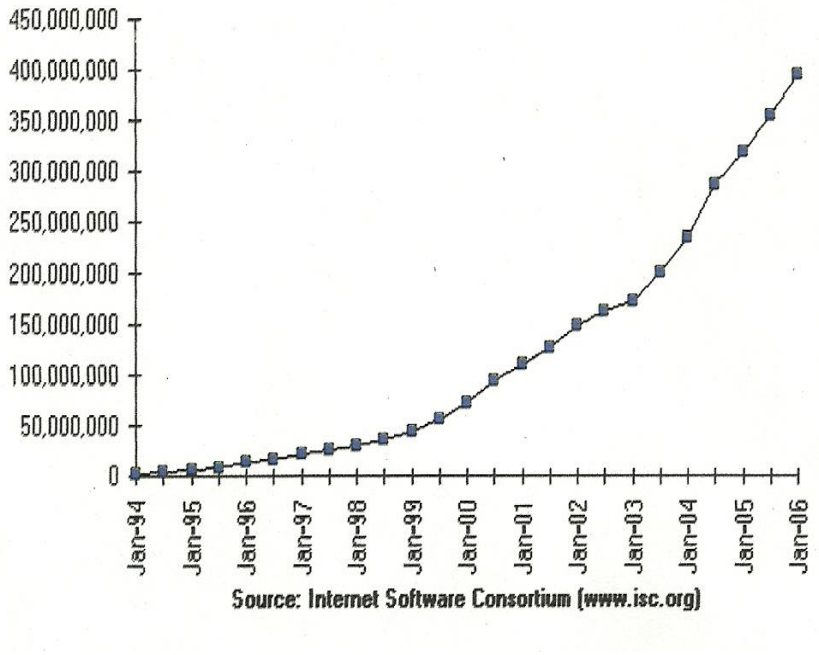

**Figure 1.1: Internet Domain Service Host Count** [11]

To sustain such a staggering growth rate, a robust security infrastructure is becoming a prerequisite for the survival of IT assets. Trends show that Computer Networks have penetrated deep into our daily life. The greater the reach and availability of the network, the greater its vulnerability to threats from within and outside the organization.

## 1.2 A Preamble to Network Security

Security is optimized by lack of access; connectivity is optimized by complete access. Internet enabled organizations; wireless connectivity and roaming clientage have made network peripheries relatively transparent. Communication has become network savvy. People are collaborating with peers in the real time, using tools for convenience rather than security. Data has started to flow iii and outside the organization through wireless media and many users request a roaming profile, so that they can access parent network even from far away places. Enterprises continue to invest heavily in perimeter security i.e. to bring security around the network, but not realizing the fact that security has to be within the network, i.e. in the network fabric itself not only at the periphery.

All the protocols, design techniques and troubleshooting methods were not defined or engineered with much thought about security because the Internet's underlying technologies were developed among a collegial group of scientists and engineers during the 1970's. There was less motivation to steal information because everyone wanted to share information. Thereby leading to adaptation of inherited architecture and a suite of protocols - as well as million lines of legacy operating systems, stacks and applications - with virtually no security infrastructure. Despite ongoing investments in anti-virus software and firewalls, enterprises remain vulnerable to attacks.

In a computer network, technological aspects are often the strongest point of defense from the outside attacks. But most attackers know that it is difficult to penetrate the periphery, so they look for easier prey. In the quest might he roaming users accessing the network and social and /or engineering methodologies to break—i.e. threat not only lies at the periphery hut might be deep rooted into the network itself. The type of threat and the means by which it gains entry to the protected assets constitute a threat vector. As per [12] the total percentage of internal threats is quoted many times higher i.e., these many computer crimes, attacks and violations originate from trusted employees as shown in Figure 1.2.

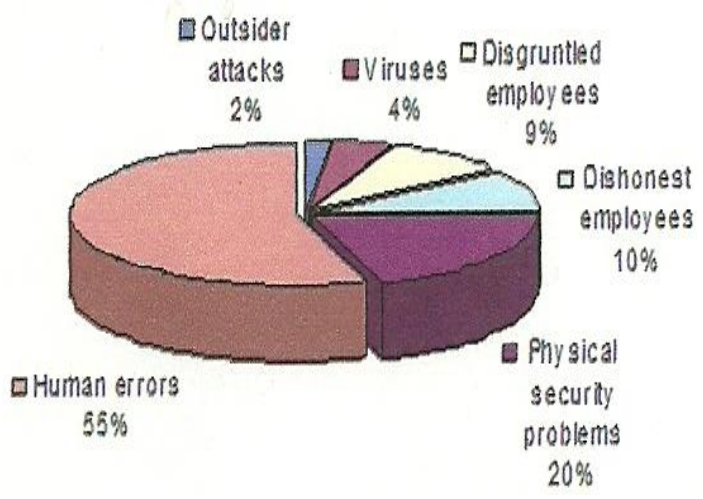


**Figure 1.2: Crime Loss Statistics** [11]

A Firewall or IDS can do nothing to protect against inside attacks. rather a firewall can provide a false sense of security, because it is common assumption that firewalls block all unwanted access, which is not completely true -firewalls allows many types of traffic to pass, some of which may he malicious. Fragmented packets or ICMP messages are tunnel through otherwise working firewall, allowing all attacker to directly access the protected resources. Dial-up modems that accept connections also contribute to internal threat vectors. E.g. Internal network is behind firewall, an ids and proxy etc. And users are not allowed the access to voice chat. These users knowingly or otherwise connect to internet for voice chats etc. Using dial up connections which completely bypasses the network security realm of an organization as shown in figure 1.3.

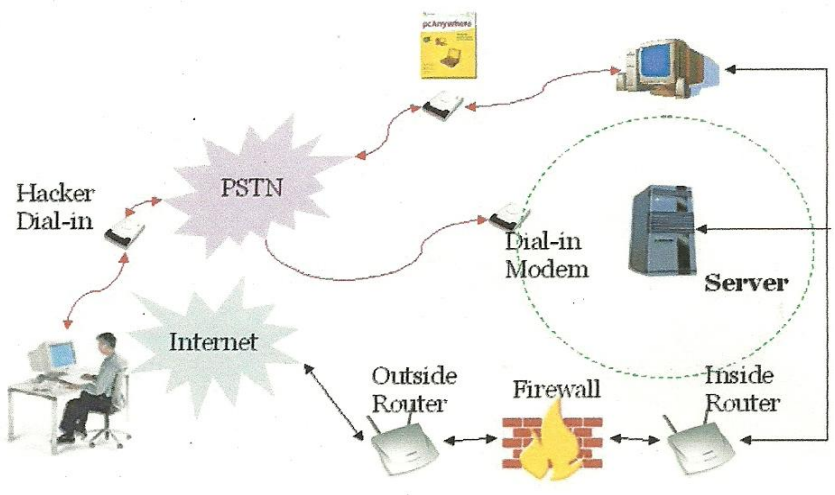


**Figure 1.3: Dial-up Connections bypassing Network Periphery Security [13]**

Dual—homed systems often configured by administration for their case to access internal as well as external network also pose a great threat to the networks. Another potential problem is use of girlfriend programs. It refers to a program handed to an employee on a floppy or CD by a trusted friend, that actually contains a Trojan program (designed to open connection on the employee's machine. They can be difficult detect and eliminate. Inside threats, although they create some of the most hazardous and ubiquitous risks to networks, are often overlooked by security strategies [13] .

Outside threat vector's most command and universal threat is the script kiddie. The script kiddie is someone looking for the easy kill. They are not out for specific information or targeting a specific company. Their goal is to gain super-user access in the easiest way possible. They do this by focusing on a small number of exploits, and then searching the entire Internet for that exploit. Sooner or later they find someone vulnerable [14]. The script kiddie methodology is a simple one. It scans the Internet for a specific weakness, when they find it, they exploit it. Most of the tools used are automated, requiring little interaction. Some of them are advanced users who develop their own tools and leave behind sophisticated backdoors. Others have no idea what they are doing and only know how to type "go" at the command prompt. Regardless of their skill level, they all share a common strategy; randomly search for a specific weakness, then exploit that weakness [14].

Every network security implementation is based on some model, which could he either specified or assumed. Mostly perimeter security models based on Firewalls and/or IDS are in uses which are reactive in nature. This model obviously with above mentioned risks lacks the robustness and provides false sense of security infrastructure. With tremendous complexity and hacking ease looming around; challenge is to build security into the network itself. This will lead to self healing and self defending network infrastructure. To achieve this, security has to he proactive i.e. should he part of the switching fabric that carries all the traffic: begin and malicious. There is compelling need to combine reactive and proactive security measures in order to have an integrated approach to the security across the information value chain. Keeping this in view, it is proposed to design and develop a proactive network surveillance framework. This Framework aims to provide learning vision to the network attacks. Objective of research work is to bring improved network security through:

- Exploring and analyzing various exploit and their detrimental effects on network security,
- exploring various honeypots and analyze their working,
- Configuring al workplace.
- development of a proactive network surveillance framework,
- creating a bootable enhanced Linux distribution with security scripts and tools (built during this work) to analyze and enhance security,
- deployment and testing of the framework,
- learning and monitoring network in real time.

The scope of the work is to enhance the security at various layers through proposed framework and specifically implement a research honeypot to uncover tools and tactics of black hat community.

## 1.3 Organization Of The Thesis

The contributions made in this thesis are organized chapter by chapter as given below:

***Chapter 2: Literature Review***

This chapter reviews the research work in the field of network security as reported in the literature. Important reactive (firewalls and IDS) and proactive (honey- pots, patching and vulnerability assessment) strategies to secure the networks are reported in this chapter. Much needed emphasis is given to the literature pertaining to Proactive strategies. Gaps have been identified and finally, based on this, problem is formulated.

***Chapter 3: Exploits and their effects***

Under this chapter various exploits and their detrimental on network security have been explored, analyzed and reported. Working of some severely clams- aging exploits is explained and countermeasures suggested. Correlation among the software engineering principles and practices and their use amongst software development community is also cited. Complete life cycle of an exploit is explained with help of live snapshots. This chapter concludes with inferences drawn and recommendations to keep exploits away from the network infrastructure.

***Chapter 4: Analysis of Honeypots***

In this chapter exploration and analysis of Open source honeypots have been done, figuring out their advantages and disadvantages. Level of interaction is other parameter which is studied in detail and analyzed. This chapter forms the basis for the design and development of 'A proactive network surveillance framework" which is described in next chapter.

***Chapter 5: Proposed Network Surveillance Framework: Design and Implementation Details***

This chapter unfolds tile design and development methodology for the said framework. A layered architecture with five layers is proposed. First layer: Core Security addresses the physical security issue and ensures that only authorized node with appropriate public-private key pair is able to access the system. This layer also recommends changes at filesystem level to enhance physical security of the installed framework. Second layer: Routing and Traffic Control offers continuous monitoring of network devices, managing bandwidth and implement access control lists to restrict the traffic entering and going out of the framework. Third layer: Security Information System focuses on reducing the complexity thereby giving intelligence to tile network. This layer generates trend reports and detailed analysis of network logs.

It identifies the malfunctioning nodes on the network sending malicious traffic, this layer also stops flooding and denial of service attacks. Fourth layer: Perimeter Security This layer recommends the placement of reactive security components with ill the network hierarchy and implements network traffic regulation rules based on various network profiles and policies. This layer also implements intrusion detection mechanism based on open-source snort. Fifth layer: Learn and Monitor the Unknown recommends operating system hardening steps, gives learning vision to the network attacks thereby monitoring the unknown entity.

***Chapter 6: Deployment, Testing of the framework and Results***

This chapter elaborates upon the deployment and testing methodology. Framework is tested against various hacking tools and techniques. Responses of the framework when deployed under various conditions are reported. Analogy is drawn with respect to existing defensive approaches. Based on the results, conclusions are reported in subsequent chapter.

***Chapter 7: Conclusion and Future Scope of the Work***

This chapter concludes the research work carried out in the thesis and final conclusions are drawn. Future scope of the work to be carried out for further enhancements is also given in this chapter.