# MCA Semester- IV

## Cryptography

## Paper Code: MCACS4T15

## Unit: 4

## System Security

# Firewall-Forensics Services

**By**

**Ms. Sushmita Chakraborty**
Assistant Professor
Dept. of MCA
Patna Women's College
Email-id: sush123.chakraborty@gmail.com

## Introduction

The goal of computer forensics is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it. Computer crime is any criminal offense, activity or issue that involves computers. Computer misuses tends to fall into two categories:

- **Computer is used to commit a crime**

  Computer pornography, threatening letters, email spam or harassment extortion, fraud and theft of intellectual property- all these crimes leave digital tracks. Investigation into these types of crimes include searching computers that are in suspected of being involved in illegal activities. Ananlysis of gigabytes of data looking for specifi keywords, happened at certain times is used in illegal activities child examining log.

- **Computer itself is a target of a crime. Computer is the victim. Computer security incident.**
  - Unauthorized or unlawful intrusions into computing system.
  - Scanning System- The systematic probing of ports to see which ones are open.
  - Denial-of-Service designed to disrupt the ability of authorized usesrs to access data.
  - Malicious code- any program or procedure that makes unauthorized actions (virus, worm, Trojan horse)

## Computer Forensics

- **Definition:** It involves obtaining and analyzing digital information often as evidence in civil, criminal, or administrative cases.
- **Computer Forensics**
  - Investigators data that can be retrieved from a computer's hard disk or other storage media.
  - Task of recovering data that users have hidden or deleted and using it as evidence.
  - Evidence can be **inculpatory**("incriminating") or **exculpatory.**
- **Examples**
  - Recovering thousands of deleted emails.
  - Performaing investigation post employment termination.

- Recovering evidence post formatting hard drive.
- Performing investigation after multiple users had taken over the system.

## Forensics

Forensic Science or forensics is the application of broad spectrum of science to answer to questions related to legal system, may be for crime or civil actions.
The use of science and technology to investigate and establish facts in criminal or civil counts of law.

## Who uses Computer Forensics?

- **Criminal Prosecutors:** Rely on evidence obtained from a computer to prosecute suspects and use as evidence.
- **Civil Litigation:** Personal and business data discovered on a computer can be used in fraud, divorce, harassment or discrimination cases.
- **Insurance companies:** Evidence discovered on computer can be used to modify cost(fraud, worker's compensation etc).
- **Private Corporation:** Obtained evidence from employee, computers can be used as evidence such as harassment, fraud and embezzlement cases.
- **Law Enforcement Officials:** Rely on computer forensics to backup search warrant and post-seizure handling.
- **Individual / Private Citizens:** Obtain the services of professional computer forensics specialists to support claims of harassment , abuse or wrongful termination from employment.
- **Computer Forensics Services:** Content, Comparison again known data. Transaction sequencing , Extraction of data, Recovering deleted data files, format conversion, keyword searching , Decrypting password, Analyzing and comparing limited source code.

## Types of Cyber Crimes

- Hacking
- Dos attack
- Virus Dissemination
- Computer Vandalism
- Piracy
- Credit Card Fraud
- Net Extortion

- Ransomware
- Pishing
- Child Pornography
- Cyber Terrorism

**Introduction to Firewall**

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

- Accept : allow the traffic
- Reject : block the traffic but reply with an "unreachable error"
- Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

## History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.

But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

## How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

**Default policy:** It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).

Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to accept, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as drop (or reject) is always a good practice.

## Generation of Firewall

Firewalls can be categorized based on its generation.

## First Generation-

- **Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).

  Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

- Incoming packets from network 192.168.21.0 are blocked.
- Incoming packets destined for internal TELNET server (port 23) are blocked.
- Incoming packets destined for host 192.168.21.3 are blocked.
- All well-known services to the network 192.168.21.0 are allowed.

## Second Generation

- **Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

## Third Generation

- **Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.
  In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

  Note: Application layer firewalls can also be used as Network Address Translator(NAT).

- **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

## Types of Firewall

Firewalls are generally of two types: Host-based and Network-based.

- **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

- **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

## Firewall Services

- **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

- **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPsec
- **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or

leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.

2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

4. A firewall can serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.