Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.264 – 270

RESEARCH ARTICLE

Simulation of Firewall Security of Cloud Server using Approach on Internet Connected System by Network Enumeration

Vivek Kumar, Nishika

Abstract: Cloud servers work in the same way as physical servers but the functions they provide can be very different. When opting for cloud hosting, clients are renting virtual server space rather than renting or purchasing physical servers.

The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet.

A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization. All cloud computing services should offer certain efficiencies to differing degrees but public cloud services are likely to be more cost efficient and scalable than private clouds.

There is threat to Cloud server security due to hacking and cracking activities of hackers and cracker. Firewall is used to make cloud server secure from these threats.

A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.

Cloud Computing

In basic terms, cloud computing is the phrase used to describe different scenarios in which computing resource is delivered as a service over a network connection (usually, this is the internet). Cloud computing is therefore a type of computing that relies on sharing a pool of physical and/or virtual resources, rather than deploying local or personal hardware and software. It is somewhat synonymous with the term 'utility computing' as users are able to tap into a supply of computing resource rather than manage the equipment needed to generate it themselves; much in the same way as a consumer tapping into the national electricity supply, instead of running their own generator.

One of the key characteristics of cloud computing is the flexibility that it offers and one of the ways that flexibility is offered is through scalability. This refers to the ability of a system to adapt and scale to changes in workload. Cloud technology allows for the automatic provision and deprovision of resource as and when it is necessary, thus ensuring that the level of resource available is as closely matched to current demand as possible. This is a defining characteristic that differentiates it from other computing models where resource is delivered in blocks (e.g., individual servers, downloaded software applications), usually with fixed capacities and upfront costs. With cloud computing, the end user usually pays only for the resource they use and so avoids the inefficiencies and expense of any unused capacity. With cloud hosting clients get the best of both worlds. Resource can be scaled up or scaled down accordingly, making it more flexible and, therefore, more cost-effective. When there is more demand placed on the servers, capacity can be automatically increased to match that demand without this needing to be paid for on a permanent basis. This is akin to a heating bill; you access what you need, when you need it, and then only pay for what you've used afterwards. Unlike dedicated servers, cloud servers can be run on a hyper visor. The role of a hypervisor is to control the capacity of operating systems so it is allocated where needed. With cloud hosting there are multiple cloud servers which are available to each particular client. This allows computing resource to be dedicated to a particular client if and when it is necessary. Where there is a spike in traffic, additional capacity will be temporarily accessed by a website, for example, until it is no longer required. Cloud servers also offer more redundancy. If one server fails, others will take its place.

Below are the key benefits of cloud servers:

- **Flexibility and scalability;** extra resource can be accessed as and when required
- **Cost-effectiveness;** whilst being available when needed, clients only pay for what they are using at a particular time
- **Ease of set up;** Cloud servers do not require much initial setup
- **Reliability;** due to the number of available servers, if there are problems with some, the resource will be shifted so that clients are unaffected.

Private Cloud

The private cloud model is closer to the more traditional model of individual local access networks (LANs) used in the past by enterprise but with the added advantages of virtualization. The features and benefits of private clouds therefore are:

- **Higher security and privacy**; public clouds services can implement a certain level of security but private clouds - using techniques such as distinct pools of resources with access restricted to connections made from behind one organization's firewall, dedicated leased lines and/or on-site internal hosting - can ensure that operations are kept out of the reach of prying eyes
- **More control**; as a private cloud is only accessible by a single organization, that organization will have the ability to configure and manage it inline with their needs to achieve a tailored network solution.
- **Cost and energy efficiency**; implementing a private cloud model can improve the allocation of resources within an organization by ensuring that the availability of

resources to individual departments/business functions can directly and flexibly respond to their demand.

- **Improved reliability**; even where resources (servers, networks etc.) are hosted internally, the creation of virtualized operating environments means that the network is more resilient to individual failures across the physical infrastructure.
- **Cloud bursting**; some providers may offer the opportunity to employ cloud bursting, within a private cloud offering, in the event of spikes in demand.

Public Cloud

Provide cloud services in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet.

The public model offers the following features and benefits:

- **Ultimate scalability**
- **Cost effective**
- **Utility style costing**
- **Reliability**
- **Flexibility**
- **Location independence**

Hybrid Cloud

A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organisation. All cloud computing services should offer certain efficiencies to differing degrees but public cloud services are likely to be more cost efficient and scalable than private clouds. Therefore, an organisation can maximize their efficiencies by employing public cloud services for all non-sensitive operations, only relying on a private cloud where they require it and ensuring that all of their platforms are seamlessly integrated.

Hybrid cloud models can be implemented in a number of ways:

- Separate cloud providers team up to provide both private and public services as an integrated service
- Individual cloud providers offer a complete hybrid package
- Organizations who manage their private clouds themselves sign up to a public cloud service which they then integrate into their infrastructure

Problem Formulation

- *Need and significance of proposed research work*
- **Security threats to Hybrid cloud servers**

- A **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.

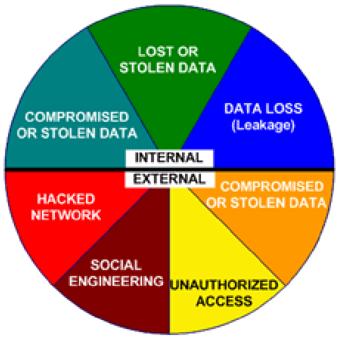
- The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community.
- While other uses of the word *hacker* exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the longstanding hacker definition controversy about the term's true meaning.
- In this controversy, the term *hacker* is reclaimed by computer programmers who argue that someone who breaks into computers, whether computer criminal (black hats) or computer security expert (white hats), is more appropriately called a **cracker** instead.
- Some white hat hackers claim that they also deserve the title *hacker*, and that only black hats should be called *crackers*.

Objective

Securing Hybrid Cloud server using firewall

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.



Security exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice.

Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking.

UDP

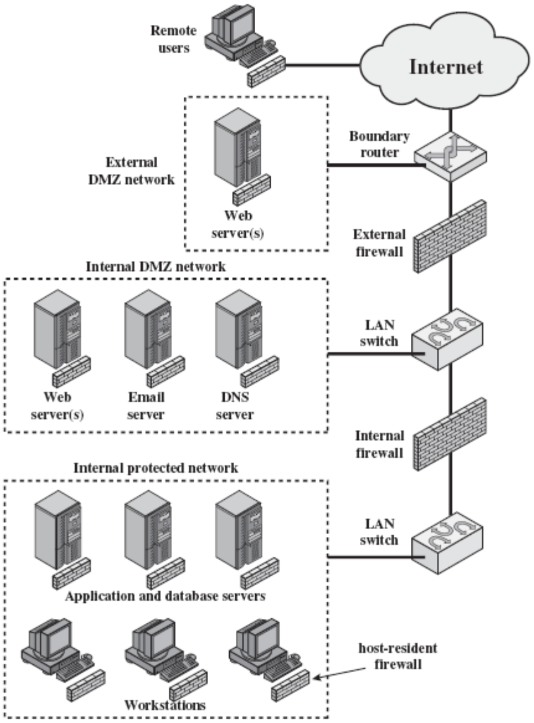
User Datagram Protocol (UDP) is part of the Internet Protocol suite used by programs running on different computers on a network. UDP is used to send short messages called datagrams but overall, it is an unreliable, connectionless protocol.

UDP network traffic is organized in the form of datagrams, which comprise one message units. The first eight bytes of a datagram contain header information, while the remaining bytes contain message data. A UDP datagram header contains four fields of two bytes each:

- Source port number
- Destination port number
- Datagram size
- Checksum

Packet filtering is also known as static filtering.

Development of firewall code is based on the following steps

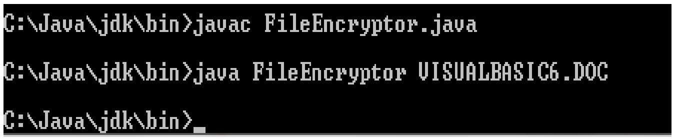


- Extract the packet header
- Check the protocol associated
- Compare with the rules

- Check the source and destination add. If protocol is same
- Check out the port if protocol is TCP
- Drop or pass the packet

Results

Step1 : Encryption



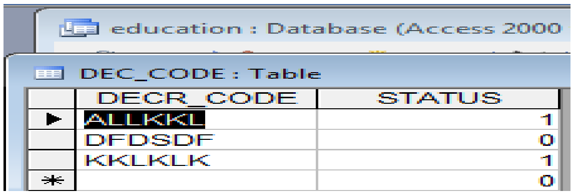
```
C:\Java\jdk\bin>javac FileEncryptor.java

C:\Java\jdk\bin>java FileEncryptor VISUALBASIC6.DOC

C:\Java\jdk\bin>_
```

Step 2: create a database “education” in ms access and create table “DEC_CODE.

STEP 3: MAKE SOME ENTRY IN DEC_CODE



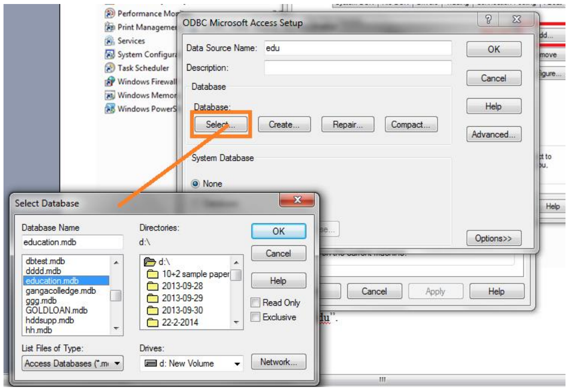
education : Database (Access 2000

DEC_CODE : Table

	DECR_CODE	STATUS
▶	ALLKKL	1
	DFDSDF	0
	KKLKLK	1
*		0

Step 4: select Microsoft access Driver and finish

Step 5: Select Database and set DSN name “edu”.



ODBC Microsoft Access Setup

Data Source Name: edu

Description:

System Database: ● None

Select Database

Database Name: education.mdb

Directories: d:\

List Files of Type: Access Databases (*.m

Drives: d: New Volume

☐ Read Only

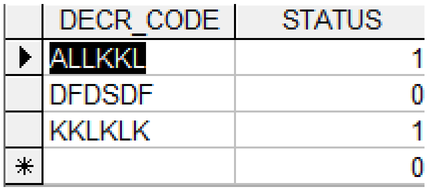
☐ Exclusive

Step 6: Decryption

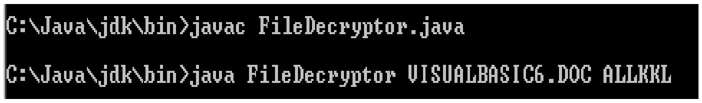
LIST OF CODES

DECRYPTION KEY CODE HAVING STATUS 1 ARE ACTIVE

DECRYPTION KEY CODE HAVING STATUS 0 ARE INACTIVE



	DECR_CODE	STATUS
▶	ALLKKL	1
	DFDSDF	0
	KKLKLK	1
*		0



```
C:\Java\jdk\bin>javac FileDecryptor.java

C:\Java\jdk\bin>java FileDecryptor VISUALBASIC6.DOC ALLKKL
```

Step : 7 remove .enc.dec extension of file and use it.

Conclusion and Future Scope

A **firewall** is a network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted.

Firewalls exist both as software to run on general purpose hardware and as a hardware appliance. Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a DHCP server for that network.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers [6] that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

References

[1] Cloud Computing
http://en.wikipedia.org/wiki/Cloud_computing
[2] Code Guru Forums. Debug assertion failed. Electronic, 2010.
[3] MSDN Forums. Blocking application that has already bound to port? Electronic, 2010.
[4] MSDN Forums. Windows driver programming and wfp. Electronic, 2010.
[5] Katie Hafner. Where Wizards Stay Up Late: The Origins of the Internet.Simon & Schuster, 1996.
[6] Gilbert Held. Cisco Security Architectures. McGraw-Hill, 1999.
[7] David Khan. Seizing the enigma: the race to break the German U-boat codes,1939-1943. Barnes & Noble, 2001.
[8] Firewalls, Tunnels, and Network Intrusion Detection http://cs.brown.edu/cgc/net.secbook/se01/handouts/Ch06-Firewalls.pdf
[9] Tennessee State Legislature. Legal resources. Electronic, 2010.FIREWALL 24/7(BPB)
[10] Logik Bomb: Hacker's Encyclopedia (1997)
[11] Hafner, Katie; Markoff, John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster. ISBN 0-671-68322-5.
[12] Sterling, Bruce (1992). *The Hacker Crackdown*. Bantam. ISBN 0-553-08058-X.
[13] Slatalla, Michelle; Joshua Quittner (1995). *Masters of Deception: The Gang That Ruled Cyberspace*. HarperCollins. ISBN 0-06-017030-1.
[14] Dreyfus, Suelette (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Mandarin. ISBN 1-86330-595-5.
[15] Verton, Dan (2002). *The Hacker Diaries : Confessions of Teenage Hackers*. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.
[16]Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. ISBN 0-8166-3345-2.