****

## SECURING OF OLDER LINUX OS

**PROJECT REPORT SUBMITTED FOR SKILL ORIENTED COURSE:**

**20IT4607 :: EHTICAL HACKING**

**JASTI VIVEK VARDHAN 208W1A1286**

**KAKUMANU CHRISTY VICTOR 208W1A1287**

**KANCHARLA PRABHU RAM 208W1A1288**

**KANTAMNENI MAHITA 208W1A1289**

****

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**V R SIDDHARTHA ENGINEERING COLLEGE**

**(AUTONOMOUS - AFFILIATED TO JNTU-K, KAKINADA)**

**Approved by AICTE &Accreted by NBA**

**KANURU, VIJAYAWADA-7**

**ACADEMIC YEAR**

**(2021-22)**

**TABLE OF CONTENTS**

**1. PROBLEM STATEMENT**

**2. SCOPE OF THE PROJECT**

**3. ARCHITECTURE/METHODOLOGY/ALGORITHM**

**4. ARCHITECTURE DESCRIPTION**

**5. IMPLEMENTATION**

**6. CONCLUSION**

**7. REFERENCES**

1. **PROBLEM STATEMENT.**

After conducting foot printing and using social-engineering techniques on the Alexander Rocco network, you have determined that the company is running several applications on Linux computers. You also discover that the payroll system runs on several Red Hat Enterprise Linux 3 (RHEL 3) servers.



Fig 1

You need to ensure that this version will be supported with patches from the vendor until the new payroll system is installed in 2011. Based on this information, write a brief report stating whether the systems can be secured until they’re replaced in 2011, and include recommendations for securing these systems.

1. **SCOPE OF THE PROJECT**

This title assists users and administrators in learning the processes and practices of securing workstations and servers against local and remote intrusion, exploitation, and malicious activity. Focused on Red Hat Enterprise Linux but detailing concepts and techniques valid for all Linux systems, this guide details the planning and the tools involved in creating a secured computing environment for the data center, workplace, and home. With proper administrative knowledge, vigilance, and tools, systems running Linux can be both fully functional and secured from most common intrusion and exploit methods.

1. **ARCHITECTURE DIAGRAM**

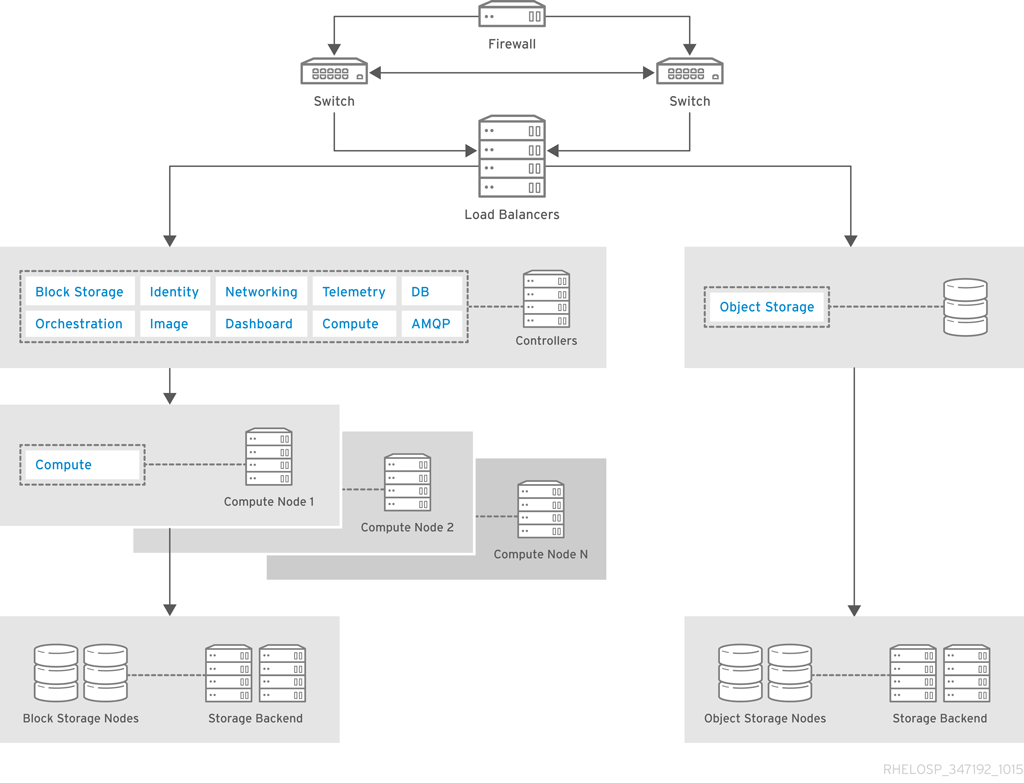


Fig 2

**3.1.ARCHITECTURE DESCRIPTION**

The architecture for this example includes three controller nodes and at least eight Compute nodes. It uses OpenStack Object Storage for static objects and OpenStack Block Storage for all other storage needs. To ensure that the OpenStack infrastructure components are highly available, nodes use the Pacemaker add-on for Red Hat Enterprise Linux together with HAProxy.

The architecture includes the following components:

* **Firewall, switches, and hardware load balancers** for the public-facing network connections.

**Fire Wall:** A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies

**Types of Fire Walls:**

* **Next-generation Firewalls (NGFW):**

A next-generation firewall (NGFW) is a [network security](https://www.cisco.com/c/en/us/products/security/what-is-network-security.html) device that provides capabilities beyond a traditional, stateful firewall. While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

* **Threat-focused NGFW:**

Next-generation firewalls (NGFWs) were created as an answer to modern security threats. NGFWs give IT solution providers and end users more visibility into their network policies and provide additional depth with regard to what users can allow or deny. However, many of these tools suffer from the same shortcomings as legacy firewalls and signature-based antivirus software—they can only detect and defend against what they “understand.”

* **Network Address Translation (NAT) Firewalls:**

A [Network Address Translation (NAT)](https://nordvpn.com/blog/what-is-nat/) firewall operates on a router to protect private networks. It works by only allowing internet traffic to pass through if a device on the private network requested it. A NAT firewall protects the identity of a network and doesn’t show internal IP addresses to the internet.

This is because, when connected to the internet, your router is assigned a single public IP address. It’s visible to the wider net and is needed to communicate with web servers. Any devices connected to the router locally have private IP addresses, which do not allow them to directly ‘communicate’ with the required web servers. This is where NAT comes into play – it directs traffic back and forth.

* **Cloud Firewalls:**

With most businesses shifting to cloud-based applications, security has evolved accordingly, leading to the introduction of cloud firewalls. Much like traditional firewalls, cloud firewalls manage the flow of information between outside domains and your internal system. Sometimes also referred to as “Next-Generation Firewalls”, these systems tackle today’s advanced threats and protect your operation’s data. As a security tool, the cloud firewall is a critical piece of infrastructure, but some platforms make deployment complicated. Not Check Point, though. Our[CloudGuard system offers rapid deployment](https://www.checkpoint.com/products/iaas-public-cloud-security/) with simple auto-scaling.

Cloud-based firewalls serve the same purpose – to prevent authorized access to private networks and cloud assets by monitoring web traffic and filtering out malicious requests based on the defined security policies.

* **Unified Threat Management (UTM) Firewalls:**

**Unified threat management, commonly abbreviated as UTM, is an information security term that refers to a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network.** A UTM appliance will usually include functions such as: antivirus, anti-spyware, anti-spam, network firewalling, intrusion detection and prevention, content filtering and leak prevention. Some units also provide services such as remote routing, network address translation (NAT), and virtual private network (VPN) support.

**Switches:** A switch is used in a wired network to connect to other devices using Ethernet cables. The switch allows each connected devices to talk to the others

**Types of Switches:**

* **KVM Switch:**

This device improves productivity, saves space, and money by allowing you to use multiple computers with one set of keyboard, monitor, and mouse. The exclusive feature offers IT administrators centralized real-time updating and maintenance. KVM switches allow users to control different IT assets (servers or desktops) from a single monitor, keyboard, and mouse, without needing to physically move those devices to the new asset.  A KVM matrix switch takes this one step further, allowing the user to operate multiple computers over multiple monitor/keyboard/mouse combinations.

* **Managed Switch:**

A managed network switch enables Ethernet devices like a PC or a network printer to communicate with each other, and provides features that let administrators configure, manage and monitor a Local Area Network (LAN). A managed network switch consequently provides administrators with more control over how data travels over the network and has access to it. A managed network switch provides a much higher Quality of Service (QoS) than an unmanaged switch. QoS features enable administrators to prioritize network traffic to ensure consistent network performance. A managed switch can, for example, prioritize delay-sensitive data like voice packets traveling over the network to make sure they don’t get dropped or delayed.

* **Unmanaged Switch:**

Unmanaged switches are plug and play devices without the need of a complex setup. These switches allow Ethernet devices to communicate with one another (such as a PC or network printer) by providing a connection to the network and passing on information to where it needs to go. They come with a fixed configuration and do not allow any changes to this configuration, therefore, there is no need for prioritising the packets. They can be desktop or rack mounted and are a less expensive option for connectivity switching needs. Unmanaged switches are mostly used to connect edge devices on network spurs, or on a small stand-alone network with only a few components. It’s suitable for any business network that wants to simplify the installation of wireless access points and IP-based surveillance cameras. They are also applicable for home use, SOHO, small businesses or to add temporary workgroups to larger networks.

* **Smart Switch:**

Smart switches are like your regular switches with a few extra handy features. They provide new ways to control your home lighting and switch wired devices. They connect through a dedicated app on your smartphone over your home Wi-Fi network so that you can access your switches anytime anywhere wirelessly. Smart switches connect to your home network providing access through Wi-Fi to remotely control the switch using a dedicated app on your smartphone. They can even be managed by a home automation controller or by using a smart speaker.

* **PoE Switch:**

A PoE switch is a network switch that has Power over Ethernet injection built-in.  Simply connect other network devices to the switch as normal, and the switch will detect whether they are POE-compatible and enable power automatically.POE switches are available to suit all applications, from low-cost unmanaged [edge switches](https://www.veracityglobal.com/products/networked-video-integration-devices/camswitch-plus.aspx) with a few ports, up to complex multi-port rack-mounted units with sophisticated management.

**Hardware load balancers:** Hardware load balancer device (HLD) is a physical appliance used to distribute web traffic across multiple network servers.

* OpenStack controller service that run Image, Identity, and Networking, combined with the support services MariaDB and RabbitMQ. These services are configured for high availability on at least three controller nodes.
* Cloud nodes are configured for high availability with the Pacemaker add-on for Red Hat Enterprise Linux.
* Compute nodes use OpenStack Block Storage for instances that need persistent storage.
* OpenStack Object Storage to serve static objects, such as images.

**4. IMPLEMENTATION**

The Red Hat Enterprise Linux 3 (RHEL 3) servers are using the common platform, thus it is upward compatible and we can apply the security patches that is applicable for upward generation this enable to achieve the up to date security even though the system run in an older version. If the vendor is updated with the security threats and the efficient patches, the RHEL 3 servers can support the patches from vendor and security can be updated.

Some of the recommendations to secure the servers

1. **Constantly Upgrade the Software and the Operating System:**



Fig 3

* A software upgrade is the newest version of the software. It usually comes with major improvements or entirely different operating systems that change or alter the application, operating system, or software drastically. A software upgrade would be adding a whole new component of security or a new feature. For example, each new iPhone usually comes with a soon-to-be-released software upgrade, and sometimes, older iPhone models can't handle them.
* Server systems and software technologies are so complicated that some of the security vulnerability they can easily go unnoticed.
* Hacker also tries to develop new and innovative ways to gain unauthorized entries into a system
* Fortunately, vendors and cybersecurity experts are constantly working to ensure that their software and operating systems are as secure as possible. Once they discover a security loophole, they will typically move quickly to have the loophole fixed.
* A software upgrade is the newest version of the software. It usually comes with major improvements or entirely different operating systems that change or alter the application, operating system, or software drastically. A software upgrade would be adding a whole new component of security or a new feature

1. **Configure Your Computer to File Backups:**

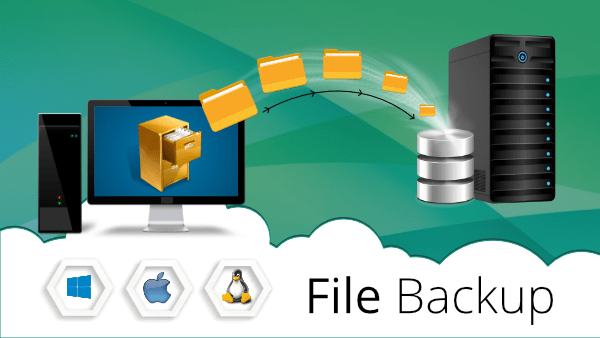


Fig 4

* You should always keep a file backup and have a restoration strategy. You never know when a hacker will succeed in breaching your servers.
* When such a breach happens, a backup file could be your savior.
* Regularly backing up your data allows you to restore all the information resources that your server held before the data breach took place.
* The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.
* File backup is a duplicate copy of your data that can be used to recover your files or even an entire hard drive after a data loss event.

**Reasons for file backup:**

**1. Data Loss Prevention**  
We’ve all heard about or experienced a tragic loss of data. The main reason for data backup is to save important files if a system crash or hard drive failure occurs.  
**2. Operation Plan B**  
There should be additional data backups if the original backups result in data corruption or hard drive failure. This option is best done via the cloud or offsite storage. Additional backups are necessary if natural or man-made disasters occur. Storms and warfare can lead to the destruction of servers and computers due to fires and floods. Luckily, we are in the age of cloud technology, where backup your data has become easier and more secure than ever before.  
**3. Tax Reporting and Audits**  
Tax authorities are notorious for audits. Laws differ among countries, but it is important for companies to save financial and accounting data for tax reporting purposes. With data backup, companies can save face during audits.  
**4. Client Relationship**  
Saved information improves client relationship management, which leads to increased marketing and sales. Additionally, saved client information builds trust and value of a company.  
**5. Investor Relations**  
Per investor relations, data backup reduces the tedious time to compile annual reports to shareholders. Saved information symbolizes a company's due diligence and organization. Without data backup, shareholders cannot make informed decisions or determine a company's value.  
**6. Archiving**  
Backed up information streamlines the development of archives. With digital information, company history is in the making.  
**7. Competitive Gain**  
Saved company data can be a competitive advantage because there are many businesses that fail to data backup important information.  
**8. Improved Productivity**  
With existing backed up files, companies improve productivity by reducing wasted time. Archived files lead to comparative studies of the past and present to devise a more effective plan.  
**9. No Wasted Time**  
Data backup reduces ‘wasted time’ by preventing repetitions. Thus, employees do not have to rewrite reports.  
**10. Peace of Mind**  
Regular data backups lead to peace of mind. In the event, a cybercrime, system crashes or disasters occur, there is a backup ready to go to restart a company's archive. It is never too late to start saving important company data. In the end, data backup is necessary to save the business from losing investors and customers and closing down.

1. **Set up Access Limitations to Your Computers files:**



Fig 5

* A user can specify access privileges to directories, networks, files, and other server elements.
* Access controls can reduce both deliberate and unintended server security breaches.
* For instance, limiting read access can help you protect confidential and private information. Similarly, restricting who can modify files and data will help maintain the integrity of the files.
* A network access restriction (NAR) is a definition, which you make in ACS, of additional conditions that you must meet before a user can access the network. ACS applies these conditions by using information from attributes that your AAA clients sent. Although you can set up NARs in several ways, they all are based on matching attribute information that a AAA client sent. Therefore, you must understand the format and content of the attributes that your AAA clients sends if you want to employ effective NARs.
* In setting up a NAR you can choose whether the filter operates positively or negatively. That is, in the NAR you specify whether to permit or deny network access, based on information sent from AAA clients when compared to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied access. Table 5-2 shows these conditions.
* One important function of network access control is limiting network access to both specific users and specific areas of the network. So, a visitor may be able to connect to the corporate network, but not access any internal resources.

1. **Install SSL Certificates:**



Fig 5

* An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection
* Secure Socket Layer certificates are security protocols that guard the communication between two systems over the internet.
* The Secure Socket Layer is a crucial element of server security. You need to ensure that any communication or data transfers between your server and clients' browsers or other servers are encrypted.
* An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser.
* Companies and organizations need to add SSL certificates to their websites to secure online transactions and keep customer information private and secure.
* In short: SSL keeps internet connections secure and prevents criminals from reading or modifying information transferred between two systems. When you see a padlock icon next to the URL in the address bar, that means SSL protects the website you are visiting.
* Since its inception about 25 years ago, there have been several versions of SSL protocol, all of which at some point ran into security troubles. A revamped and renamed version followed — TLS (Transport Layer Security), which is still in use today. However, the initials SSL stuck, so the new version of the protocol is still usually called by the old name.
* SSL works by ensuring that any data transferred between users and websites, or between two systems, remains impossible to read. It uses encryption algorithms to scramble data in transit, which prevents hackers from reading it as it is sent over the connection. This data includes potentially sensitive information such as names, addresses, credit card numbers, or other financial details.
* When a website is secured by an SSL certificate, the acronym HTTPS (which stands for HyperText Transfer Protocol Secure) appears in the URL. Without an SSL certificate, only the letters HTTP – i.e., without the S for Secure – will appear. A padlock icon will also display in the URL address bar. This signals trust and provides reassurance to those visiting the website.

1. **Use Virtual Private Networks (Private Networking):**



Fig 6

* VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks.
* VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data.
* Private networks are based on Internet Protocol address space. A VPN is said to be private because no Internet Protocol packets addressed are transmitted via a public network.
* A VPN will allow you to create a connection between different computer devices located in different places. It lets you to carry out operations on your servers in a secure manner.
* A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.
* A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.
* **Secure encryption:** To read the data, you need an encryption key . Without one, it would take millions of years for a computer to decipher the code in the event of a [brute force attack](https://www.kaspersky.com/resource-center/definitions/brute-force-attack) . With the help of a VPN, your online activities are hidden even on public networks.
* **Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.
* **Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing**, you can switch to a server to another country and effectively “change” your location.
* **Secure data transfer:** If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

1. **Server Password Security:**



Fig 7

* When it comes to server security, make sure you use password best practices.
* The first step is to develop clear password policies and rules that all members using the server should follow. You should enforce minimum character length for passwords, set password complexity guidelines, enable session timeout for inactivity, and use a multiple-factor authentication strategy.
* It's also useful to have a clear password expiration policy. Passwords should only be allowed to last a few weeks or months. It's best to encourage all users to implement safe password storage to avoid passwords landing in unsafe hands.
* Instead of a password, you can [authenticate an SSH server using a pair of SSH keys](https://phoenixnap.com/kb/generate-setup-ssh-key-ubuntu), a better alternative to traditional logins. The keys carry many more bits than a password and are not easily cracked by most modern computers. The popular RSA 2048-bit encryption is equivalent to a 617-digit password.
* The key pair consists of a public key and a private key.
* The public key has several copies, one of which remains on the server, while others are shared with users. Anyone that has the public key has the power to encrypt data, while only the user with the corresponding private key can read this data. The private key is not shared with anyone and must be kept secure. When establishing a connection, the server asks for evidence that the user has the private key, before allowing [privileged access](https://phoenixnap.com/blog/privileged-access-management).
* Secure your web administration areas and forms with **Secure Socket Layer (SSL)** that guards information passed between two systems via the internet. SSL can be used both in server-client and in server-server communication.
* The program scrambles data so that sensitive information (such as names, IDs, credit card numbers, and other personal information) is not stolen in transit. Websites that have the [SSL certificate](https://phoenixnap.com/kb/openssl-tutorial-ssl-certificates-private-keys-csrs) have HTTPS in the URL, indicating they are secure.
* Not only does the certificate encrypt data, but it is also used for user authentication. Therefore, by managing certificates for your servers, it helps establish user authority. Administrators can configure servers to communicate with centralized authority and any other certificate that the authority signs.
* Another way to ensure secure communication is to use private and virtual private networks (VPNs), and software such as OpenVPN (see our guide on [installing and configuring OpenVPN on CentOS](https://phoenixnap.com/kb/openvpn-centos)). Unlike open networks which are accessible to the outside world and therefore susceptible to [attacks from malicious users](https://phoenixnap.com/blog/cyber-security-attack-types), private and virtual private networks restrict access to selected users.
* Private networks use a private IP to establish isolated communication channels between servers within the same range. This allows multiple servers under the same account to exchange information and data without exposure to a public space.

1. **Use Firewall Protection:**



Fig 8

* Firewalls are a must-have to ensure that your servers are safe. They filter incoming and outgoing traffic to allow only specific services and lockout unsafe ones.
* There are a few different classifications of firewalls. The first group deals with the public services that anyone on the internet anonymously accesses.
* The second is the private services that a select group of authorized accounts can access. The last is the internal services that require no exposure to the outside world.
* You should restrict access to these services depending on which group fits the situation. You should configure your server to refuse all accesses except those that are mandatory to your servers
* Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e., computer network addresses), applications, or ports while allowing relevant and necessary data through.
* Categories of firewalls include hardware and software. While both have advantages and disadvantages, the decision to use a firewall is more important than deciding which type you use.

**Hardware** – Typically called network firewalls, these physical devices are positioned between your computer and the internet (or other network connection). Many vendors and some internet service providers (ISPs) offer integrated small office / home office routers that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers and controlling the network activity that attempts to pass through them. The advantage of hardware-based firewalls is that they provide an additional line of defense against attacks reaching desktop computing systems. The disadvantage is that they are separate devices that require trained professionals to support their configuration and maintenance.

**Software** – Most operating systems (OSs) include a built-in firewall feature that you should enable for added protection, even if you have an external firewall. Firewall software is also available separately from your local computer store, software vendor, or ISP. If you download firewall software from the internet, make sure it is from a reputable source (i.e., an established software vendor or service provider) and offered via a secure site. (See [Understanding Website Certificates](https://www.cisa.gov/uscert/ncas/tips/ST05-010) for more information.) The advantage of software firewalls is their ability to control the specific network behavior of individual applications on a system. A significant disadvantage of a software firewall is that it is typically located on the same system that is being protected. Being located on the same system can hinder the firewall’s ability to detect and stop malicious activity. Another possible disadvantage of software firewalls is that—if you have a firewall for each computer on a network—you will need to update and manage each computer’s firewall individually.

**5. CONCLUSION**

Now we have learned about the origins, reasons, and aspects of security, we can determine the appropriate course of action with regard to Red Hat Enterprise Linux. It is important to know what factors and conditions make up security in order to plan and implement a proper strategy. With this information in mind, the process can be formalized and the path becomes clearer as you delve deeper into the specifics of the security process.

**6. REFERENCES**

[1] [https://access.redhat.com/documentation/en- us/red\_hat\_enterprise\_linux\_openstack\_platfor m/7/html/architecture\_guide/examples](https://access.redhat.com/documentation/en-%20us/red_hat_enterprise_linux_openstack_platfor%20%20%20%20%20%20%20%20m/7/html/architecture_guide/examples)

[2] [What Is a Next-Generation Firewall (NGFW)? - Cisco](https://www.cisco.com/c/en_in/products/security/firewalls/what-is-a-next-generation-firewall.html)

[3]<https://access.redhat.com/documentation/enus/red_hat_enterprise_linux_openstack_platform/7/html/architecture_guide/examples>

[4] [What is VPN? How It Works, Types of VPN (kaspersky.com)](https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn)

[5] [Understanding Firewalls for Home and Small Office Use | CISA](https://www.cisa.gov/uscert/ncas/tips/ST04-004#:~:text=Firewalls%20provide%20protection%20against%20outside,or%20network%20via%20the%20internet.)

[6] [Server Security Tips – Secure Your Server with These Best Practices (freecodecamp.org)](https://www.freecodecamp.org/news/server-security-tips/#:~:text=Server%20Password%20Security&text=You%20should%20enforce%20minimum%20character,a%20clear%20password%20expiration%20policy.)