REV. INVESTIG. ALTOANDIN

REPORTE DE CASO

Rev. Investig. Altoandin. 2016; Vol 18 Nº 4: 475 - 482

http:huajsapata.unap.edu.pe/ria - http://dx.doi.org/10.18271/ria.2016.240

Octubre - Diciembre - ISSN: 2306-8582 (Versión impresa)
ISSN: 2313-2957 (Versión digital)

Journal of High Andean Research
VOL 18 Nº 4
Revista de Investigaciones Altoandinas

Determine the operation of a firewall to block avoidance internet censorship systems based on proxy

Diseño de un cortafuegos para bloquear sistemas de evasión de censura de internet basados en proxy

[1,4] Christian Augusto Romero Goyzueta, [2,4] Ferdinand Edgardo Pineda Ancco, [3,4] Jesús Vidal Lopez Flores

[1,2,3,4]Docente de la Escuela
Profesional de Ingeniería Electrónica de la Universidad Nacional del Altiplano, Puno - Perú Correspondencia: [1]romeroc24@gmail.com, [2]ferpineda@gmail.com, [3]jlovidal@gmail.com

ARTICLE INFO

Article received 30-09-2016
Article accepted 12-12-2016
On line: 20-12-2016

PALABRAS CLAVES:

ultrasurf,
torbrowser,
security policies,
network security.

ABSTRACT

Within the policies of an organization is possible find not to allow users to access sites on the Internet for entertainment or social networks, as in the case of production organizations and educational therefore a firewall that is used implemented certain rules based on the policies of the organization, blocks access to certain defined sites while you let others free. However there is no implemented rules to block proxies of Avoidance Internet Censorship Systems, the user can access easily to those proxies. The addresses of these proxies change very frequently, so it is almost impossible to block them all, and eventually they appear more. The proposed solution is to create a firewall that uses dynamic rules, these rules are created for the dynamic firewall. A test of each address to a destination is made and if it finds that the destination is a proxy of one of these evation systems; the firewall creates a new rule and automatically implemented. In this way the user will lose access to the proxy.

INFORMACIÓN DEL ARTÍCULO

Artículo recibido 30-09-2016
Articulo aceptado 12-12-2016
On line: 20-12-2016

KEY WORDS:

ultrasurf,
torbrowser,
políticas de seguridad,
seguridad de red.

RESUMEN

Dentro de las políticas de una organización podría encontrar el no permitir que los usuarios accedan a sitios en Internet para el entretenimiento o las redes sociales, como en el caso de las organizaciones de producción y educativas, por tanto, un firewall o cortafuegos utiliza ciertas reglas en base a las políticas de la organización, bloquea el acceso a ciertos sitios definidos, mientras deja los demás libres. Sin embargo, como no se ha implementado reglas para bloquear proxies de Sistemas de Evasión de Censura de Internet, el usuario puede acceder a los proxies fácilmente. Las direcciones de estos servidores proxy cambian con mucha frecuencia, por lo que es casi imposible de bloquear a todos ellos, y con el tiempo aparecen más. La solución propuesta es la creación de un cortafuegos que utiliza reglas dinámicas, estas reglas las crea el firewall. Una prueba de cada dirección a un destino se hace, y si comprueba que el destino es un proxy de uno de estos sistemas de evasión; el cortafuegos crea una nueva regla y se aplica de forma automática. De esta manera el usuario perderá el acceso al proxy.

INTRODUCTION

The rules implemented in a firewall in order to block access to certain sites on the Internet, are entered by the administrator and remain until the administrator decides to make updates or changes (Smith, 2011). Users have found a way to prevent the firewall blocks access to sites not permitted by the organization, making the use of avoidance Internet censorship systems, as the case of Ultrasurf, Tor Browser or Proxy for Chrome (Adelstein, 2007). This avoidance system works by running software on the client that allows the user to connect to a proxy, usually a HTTP Proxy, and not connecting the user directly to the desired website. The proxy located somewhere in the world receives user requests and redirects data from there to the desired user sites (Bhargava, 2016).

The existing problem is that the policies of the organization are broken and the low productivity of the working groups which have free access to the Internet, despite implementing a corporate firewall that denies access to certain sites on the Internet.

We are using iptables is a user program that allows a system administrator to configure the tables provided by the Linux kernel firewall implemented by different Netfilter modules. Different kernel modules and programs are currently used for different protocols such as IPv4, IPv6, ARP and Ethernet frames (Van Vugt, 2013). This way you can manage the tables for certain protocol and allow, reject or ignore packets entering, pass or leave the system (Firewall). For example, you can configure an IPv4 packet is rejected as it leaves the Firewall. This way you can describe the actions that are governed by rules in the Firewall as follows (Lammle, 2013).

- (Permit), this rule allows a packet is processed without restrictions.
- (Reject), this rule makes a package is rejected and an error notification is displayed to the user.
- (Drop), this rule rejects the package silently, i.e. not notify the user in any way about the action taken.
- (Input) is an action taken when the packet enters a network interface.
- (Forward), the action is taken when the packet passes through the system, i.e., as entered by a network interface but not yet out of the system.
- (Output), the action is taken when the packet exits through a network interface system.

Another tool is bash and is a command processor that typically runs in a text window, where the user types commands that cause actions. Bash can also read commands from a file, called a script (Van Vugt, 2008). Like all Unix shells, it supports filename globbing (wildcard matching), piping, here documents, command substitution, variables and control structures for condition-testing and iteration. The keywords, syntax and other basic features of the language were all copied from sh. Other features, e.g., history, were copied from csh and ksh. Bash is a POSIX shell, but with a number of extensions (Lammle, 2014).

Expect, will help us like an extension to the Tcl scripting language written by Don Libes, is a program to automate interactions with programs that expose a text terminal interface. Expect was originally written in 1990 for Unix systems, but is now also available for Microsoft Windows and other systems. It is used to automate control of interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, ssh, and others. Expect uses pseudo terminals (Unix) or emulates a console (Windows), starts the target program, and then communicates with it, just as a human would, via the terminal or console interface. Tk, another Tcl extension, can be used to provide a GUI (Madummala, 2016).

MATERIALS AND METHODOLOGY

2.1. Objectives

Determine the operation of a firewall with dynamic rules to block avoidance Internet censorchip systems based on proxy.

2.2. Hypothesis

A firewall with dynamic rules will permit to block avoidance Internet censorchip systems based on proxy.

2.3. Research Design

Experiments are most effective for explanatory research and are often limited to topics in which you can manipulate the situation where people are. In such experiments, it divides people under investigation in two. This research is experimental because it is a type of research that uses logic and principles found in the natural sciences. Experiments can be performed in the laboratory or in real life. Here a relatively small number of individuals or teams involved and address a very focused question.

2.4. Level Research

It is explanatory, by manipulating the independent variable, to see the effect that has on the dependent variable.

2.5. Type Of Investigation

The type is descriptive because is necessary the description of practical use of knowledge and theories networks of firewalls in order to improve and solve the specific problem called avoidance Internet censorchip systems based on proxy.

2.6. Space and Time

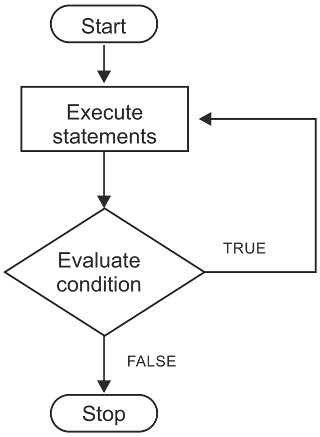
The research was made from June 2nd to Setember 13th 2016 on the Cisco Academy Laboratory, of the Electronics Engineering Department of the Universidad Nacional del Altiplano; on Puno, Perú.

2.7. Techniques and Tools

- Techniques

The technique used was the playtesting, that is a technique of improve the software with the progress of the research and each iteration. This technique is so simple like a while operation, every iteration evaluate the condition, if the condition is true, the system can be improved but if is false the stop is used to start again from the initial reference.

Fig. 1. The algorithm of playtesting described as a simple while operation.



Source: Van Vugt, 2008.

- Instruments

The instrument is the test, the researcher takes steps to evaluate the behavior of the system.

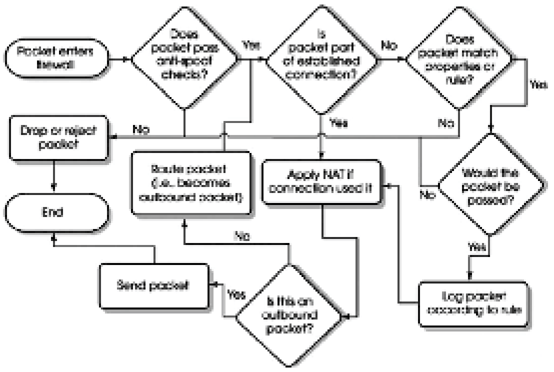
- Data Collection Plan

The following steps for data collection followed:

✓ Scan datagrams on Wireshark.

✓ Scan datagrams on tcpdump.

Fig. 2. The algorithm of the firewall.


Packet enters firewall
Does packet pass anti-spoof checks?
Yes
Is packet part of established connection?
No
Does packet match properties of rule?
Yes
Drop or reject packet
No
Yes
No
Route packet (i.e., becomes outbound packet)
Apply NAT if connection used it
Would the packet be passed?
No
End
No
Yes
Send packet
Yes
Is this an outbound packet?
Log packet according to rule

Source: Lammle, 2013.

- *Plan* Data Processing

The main purpose of the research is test the proxy base on the web contents.

- *Hardware:*

✓ Desktop PC (Laptop S55-B).

✓ Server Power Edge R620.

- *Software:*

✓ 64-bit Operating System Windows 8.1 Professional.

✓ Linux Operating System: Ubuntu Server 14.04.1 LTS.

- ✓ VirtualBox 4.3.20.
- ✓ Wireshark.
- ✓ Tcpdump.
- ✓ Ultrasurf.
- ✓ Tor Browser.
- ✓ Chrome proxies.

RESULTS

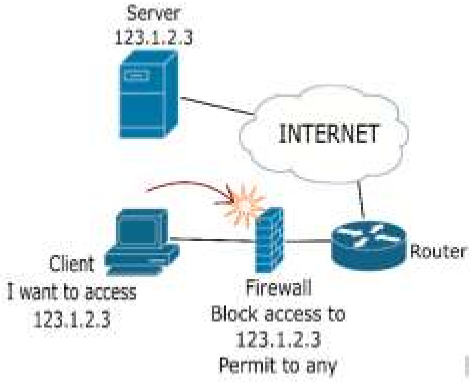
There are many features and functions that a firewall can assume. A method to block access to certain IP addresses and allow access to any other IP addressescan be use. For example another method that is opposite to the above, what it does, is allow access to certain IP addresses while blocking access to the rest or any other IP addresses, the latter method can even block avoidance Internet censorship systems, but has a very big disadvantage; both methods are described below.

3.1. *Block access to certain IP addresses and allow access to the rest*

This method is quite to use, because it is very useful for organizations that want access to all Internet sites except some sites, such as whether you want users should not access social networks as facebook.com, but if they can access pages from around the world to do research.

To achieve this configuration on firewall, add rules to block sites and allow access to any other site (Mauerer, 2008).

Fig. 3. A client is trying to access a prohibited site and is blocked by the firewall.

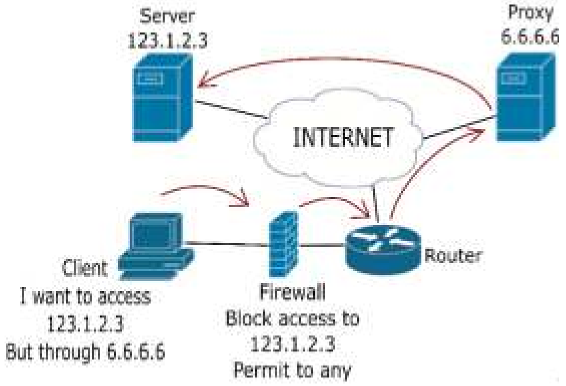


Source: Authors.

The problem with this method is that the avoidance Internet censorchip systems based on proxy based on proxy can easily hack it.

This happens in the following way, the user does not directly access a site blocked by the firewall, the user accesses a proxy that has an address that the firewall is not blocking, then this proxy redirects the connection to the real destination. In this way the user avoid the firewall without problems (Negus, 2009).

Fig. 4. A client can use a proxy to avoid the firewall.

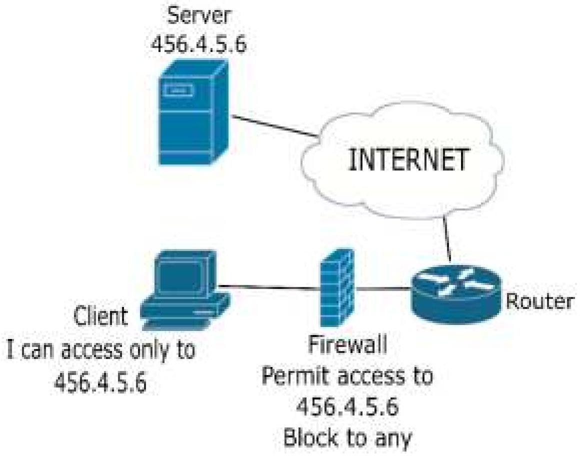


Source: Authors.

3.2. *Allow access to certain sites and block access to all other Internet*

This method is very useful especially to block the Avoidance Internet censorchip systems based on proxy based on proxy, because a user is able to access certain sites allowed by the firewall and all the rest of the Internet, including proxy, are blocked (Negus, 2013).

Fig. 5. A client can only Access to one or a few sites and any other Access is blocked.

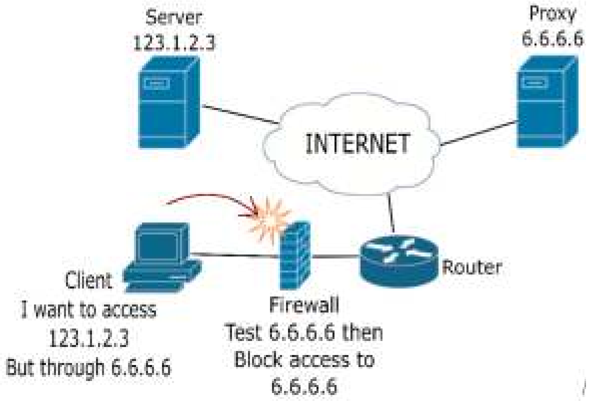


Source: Authors.

The problem with this method is that users cannot access more than a few sites on the Internet, and would not have the flexibility to explore or investigate on Internet (Saini, 2011).

The firewall with dynamic rules, in this research, is characterized by the ability to test a website and if this site is a proxy, then it is blocked, if is a common web site, it is allowed.

Fig. 6. Firewall can test a site and block it if is a proxy.



Source: Authors.

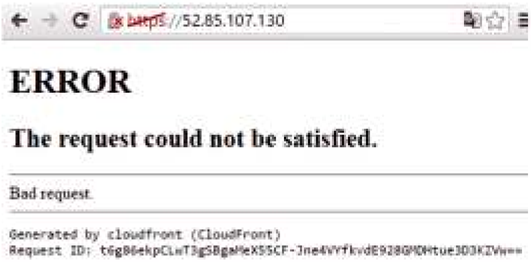
3.3. Implementing Dynamics Rules

Dynamic rules are not implemented by the user, who implements is the firewall. Is based on a test that is done to the destination. The firewall can have static rules previously entered by the user and the firewall will add more rules later.

This is where the use of bash scripting and expect is done, because they automate process methods and commands on GNU/Linux. Bash allows you to enter commands into the operating system, and expect allows you to enter commands in response to certain outputs returned by the operating system.

This is the web output of a proxy server for Intenet censorship avoidance systems.

Fig. 7. The web output of a proxy server for avoidance Internet censorchip systems based on proxy.



ERROR

The request could not be satisfied.

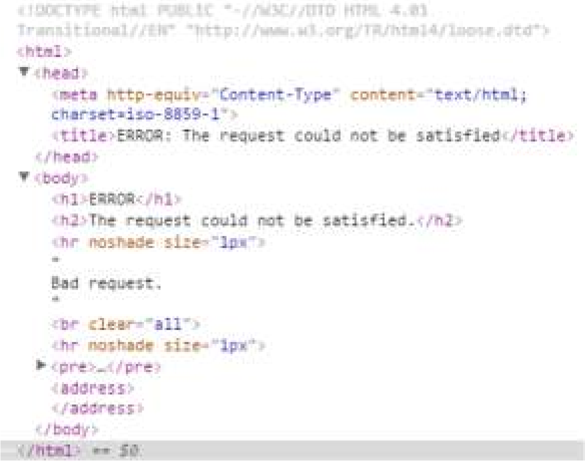
Bad request.

```
Generated by cloudfront (CloudFront)
Request ID: t6g86ekpCLwT3gSBgaMeX55CF-Jne4VYfkvdE928GMDHtue3D3KZVw==
```

Source: Authors.

The firewall will compare this web output with a common web and determine if is a proxy server for Avoidance Internet censorchip systems based on proxy. The firewall can use the html code and other methods to search proxy servers.

Fig. 8. The html web output of a proxy server for avoidance Internet censorchip systems based on proxy.

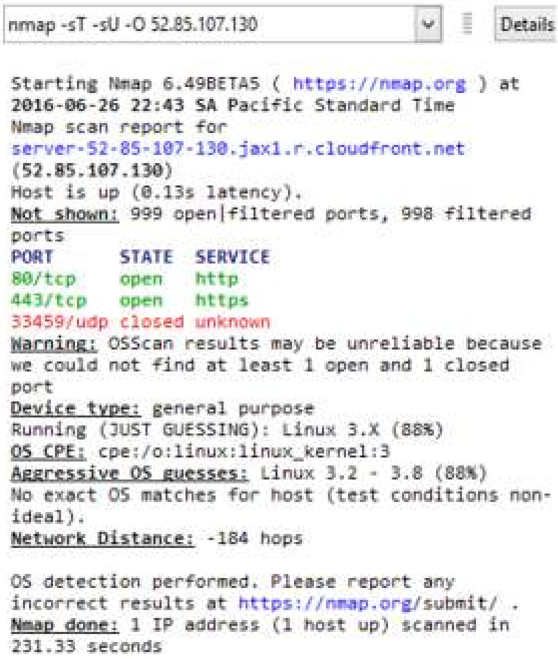


```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
▼<head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=iso-8859-1">
    <title>ERROR: The request could not be satisfied</title>
  </head>
▼<body>
    <h1>ERROR</h1>
    <h2>The request could not be satisfied.</h2>
    <hr noshade size="1px">
    "
    Bad request.
    "
    <br clear="all">
    <hr noshade size="1px">
  ▶<pre>…</pre>
    <address>
    </address>
  </body>
</html> == $0
```

Source: Authors.

The nmap scan of a proxy server can show us the ports available and other data that can be tested. For example the next output show us that this proxy server is a linux server with open ports 80 (http) and 443 (https) to make the test operations. The firewall can test both ports and determine if is a common web page or if is a proxy.

Fig. 9. The nmap scan of a proxy server for avoidance Internet censorchip systems based on proxy.



```
Starting Nmap 6.49BETA5 ( https://nmap.org ) at
2016-06-26 22:43 SA Pacific Standard Time
Nmap scan report for
server-52-85-107-130.jax1.r.cloudfront.net
(52.85.107.130)
Host is up (0.13s latency).
Not shown: 999 open|filtered ports, 998 filtered
ports
PORT      STATE  SERVICE
80/tcp    open   http
443/tcp   open   https
33459/udp closed unknown
Warning: OSScan results may be unreliable because
we could not find at least 1 open and 1 closed
port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 3.2 - 3.8 (88%)
No exact OS matches for host (test conditions non-
ideal).
Network Distance: -184 hops

OS detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in
231.33 seconds
```

Source: Authors.

DISCUSSION

Bhargava on 2016 says: "The impact of firewall security rule base in controlling transmission of malicious objects is analyzed. We are taking firewall security as a media coverage factor in our computer network model of malicious code propagation. Asymptotic local stability method is used as an alternate to find the stability of the system. Finally, a sensitivity analysis of the system parameters for basic reproduction number and endemic equilibrium points has been carried out using normalized forward sensitivity index. Numerical experimentation has been carried out to simulate the system of equations in support of analytical findings". In the research the main purpose is test the proxy base on the web contents and not to simulate the system of equations in support of analytical findings or made the sensitivity analysis of the system parameters for basic reproduction number, the results were that can be possible to block systems like ultrasurf and torbrowser, is not necessary the use of a simulator because those models are not published and its behavior can not be determine on a simulator.

Maddumala on 2016 says: "Firewalls are the first line of defense in cyber-security. They prevent malicious and unwanted network traffic entering the perimeters of organizations. The strength of a firewall lies in its policy configuration which is also a crucial task for any security administrator. The scope of Firewall policies have been expanding to address ever changing security requirements of an organization. In this process, new security parameters have been researched and one such parameter is temporal policy. Firewall temporal policy is a firewall policy that allows or denies a network packet based on specified day and time range of the policy in addition to the packet filtering rules. Firewall vendors such as CISCO and Palo Alto have already featured firewall temporal policies in their security products. Inclusion of temporal policies in firewall policies results in additional overhead for storing and scanning Firewall policies. As temporal policies are represented in week days and time, they consume considerable amount of space. In this paper, we present an innovative and efficient method for representing temporal policies which includes compact representation of temporal policies and detection of anomalies using set operations. Our approach significantly reduces the storage requirement and improves the scanning functionality of firewall. We also present a new method of creating policy sets based on week days". The research describes how is possible to block the undesired proxy sites permanently as posible and not to make temporal policies that are represented in week days and time, the advantage of the research is the funtionality of the firewall to achieve the objectives and not to describe or develop the policies in the firewall. Every iteration can be an improve of the description of the firewall.

CONCLUSIONS

Every iteration on the process can find the best way to determine the operation to block avoidance Internet censorship systems based on proxy, all the process in this research is based on the web content but other methods can be determine later. A user can access banned sites on duration of the test, but once the firewall identifies that the destination, the access is denied to the site immediately. Bash and expect automate all processes to implement dynamic rules in the firewall. GNU/Linux is a great choice for its flexibility, performance and low cost of implementation. The difference against a common firewall is the dinamyc creation of the policies and rules by the firewall and not by the human admninistrator. To achieve this, the firewall needs high processing capacity, which is get it with a very affordable processor on the market, it then proceeds to perform the test and finally automation allows it to add firewall rules by itself.

ACKNOWLEDGEMENTS

We thank our good friends, families and our university who help us at all times.

BIBLIOGRAPHIC REFERENCES

Adelstein, T & Lubanovic, B. (2007). Linux System Administration. United States of America, O'Reilly Media Inc.

Bhargava, A.; Kumar, D.; Jain, P. and Dhar, J. (2016). Dynamics of attack of malicious codes on the targeted network: Effect of firewall. IEEE Xplore. Visited September 20th on http://ieeexplore.ieee.org/document/7569534/

Lammle, T. (2014). CCNA/CCENT IOS Commands Survival Guide: Exams 100-101, 200-101, and 200-120 2nd Edition. United States of America, Sybex.

Lammle, T. (2013). CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120 1st Edition. United States of America, Sybex.

Maddumala, M. & Kumar, V. (2016). Efficient Determine the operation of a firewall Temporal Policies. IEEE Xplore. Visited September 20th on http://ieeexplore.ieee.org/document/7552253/

Mauerer, W. (2008). Professional Linux Kernel Architecture. United States of America, Wiley Publishing Inc.

Negus, C. (2013). Ubuntu Linux Toolbox 2nd ed. United States of America, John Wiley & Sons.

Negus, C. (2009). Linux Bible. United States of America, Wiley Publishing Inc.

Saini, K. (2011). Squid Proxy Server 3.1. United States of America, Packt Publishing.

Smith, R.W. (2011). LPIC-2 Linux Professional Institute Certification. United States of America, Wiley Publishing Inc.

Smith, R.W. (2011). LPIC-1 Linux Professional Institute Certification 2nd ed. United States of America,Wiley Publishing Inc.

Van Vugt, S. (2013). Red Hat Enterprise Linux 6 Administration. United States of America, John Wiley & Sons.

Van Vugt, S. (2008). Beginning Ubuntu LTS Server Administration: From Novice to Professional 2nd ed. United States of America, Apres.