Gema Wiralodra

Publication details, including instructions for authors and subscription information:
https://gemawiralodra.unwir.ac.id

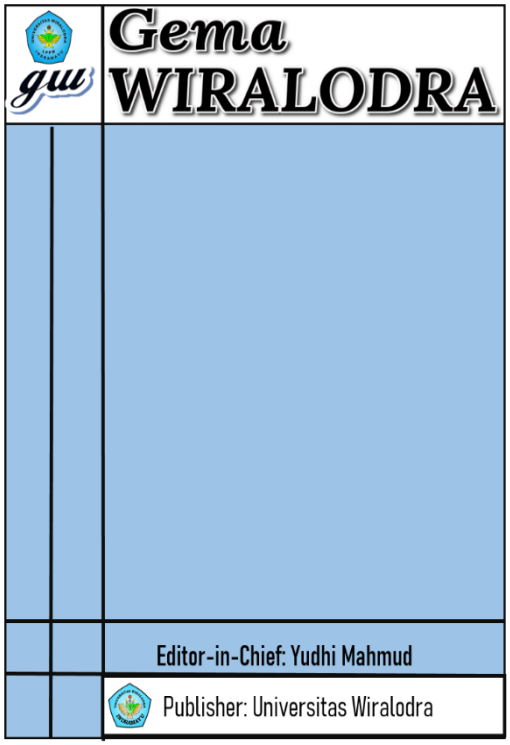


Image based Ubuntu operating system using packer solutions

Elfrin Erawan[a*], Muhammad Salman[b]
[a]Department of Electrical Engineering, Universitas Indonesia, Indonesia, elfrin.erawan@ui.ac.id
[b]Department of Electrical Engineering, Universitas Indonesia, Indonesia, muhammad.salman@ui.ac.id

To cite this article:
Erawan, E & Salman, M. (2023). Image based Ubuntu operating system using packer solutions. *Gema Wiralodra*, *14*(2), 961-968.
To link to this article:
https://gemawiralodra.unwir.ac.id/index.php/gemawiralodra/issue/view/22
Published by:
Universitas Wiralodra
Jln. Ir. H. Juanda Km 3 Indramayu, West Java, Indonesia

Gema Wiralodra, 14(2), 961-968
https://gemawiralodra.unwir.ac.id/index.php/gemawiralodra
p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Orginal Article

Image based Ubuntu operating system using packer solutions

Elfrin Erawan[a*], Muhammad Salman[b]
[a]Department of Electrical Engineering, Universitas Indonesia, Indonesia, elfrin.erawan@ui.ac.id
[b]Department of Electrical Engineering, Universitas Indonesia, Indonesia, muhammad.salman@ui.ac.id

*Correspondence: elfrin.erawan@ui.ac.id
Submit 27-05-2023, accepted 15-08-2023, published 16-08-2023

Abstract
System frequent Linux operations are used on critical systems. Part systems big pay attention to safety and reliability. Ubuntu Linux is one of all Lots common Linux distributions used for system server operation. To improve security on Ubuntu Linux is required to strengthen the security system process. Strengthening security system operation is one solution for the system operation more stand to attacks and vulnerabilities. *Center for Internet Security* (CIS) is one caring organization for cyber security and provides *benchmarks* for configuration system safe Ubuntu operation. *Benchmarks* cover recommended settings for various component systems like file permissions, application, configuration networking, logging, and management of users. The study aims to improve security system operation with the use of control strengthening security based on *CIS Benchmark* v1.1.0 servers' level 2 with the automatic model use packers application. The developed methodology consists of four phases. The first phase is Packer server installation and configuration. The second phase is to build a configuration base Ubuntu installation with user *data*. The third phase is the application *Ansible playbook* in *runtime* Packer automation for automation reinforcement at the time of installation and produces *image* virtual machine. In phase, lastly, apply structure using *image* virtual machine-generated and verified percentage reinforcement and optimization achieved. After strengthening security, use research methods. This generated a score conformity audit of 218 controls or 99.54% of the total 219 CIS Benchmark controls.
Keywords: Automation, CIS, Security, Packer, Reinforcement, Ubuntu

1. Introduction

System frequent Linux operations are used on critical systems Because of known will stability, security, and reliability (Husaini et al., 2015). Linux is an open-source system that delivers discretion to its users and will control them completely to approach them, so it is suitable for critical systems where reliability and security are essential (Kleidermacher & Kleidermacher, 2012). Additionally, linux has a strong community of developers constantly working to improve system performance, safety, and reliability (Feller & Fitzgerald, 2000). This community-driven development approach ensures critical Linux-based systems are continuously updated with the latest security patches and features.

Different Linux distributions are available, especially for server purposes, each with features and benefits. However, some of the most popular Linux distributions for servers (Chuyko, 2022) include Ubuntu server, Debian server, Red Hat Enterprise Linux (RHEL), CentOS, and Amazon Linux 2. When using configuration default, Linux servers may give optimal security directly. To ensure maximum security, linux system administrators must apply the best and tight systems practices to configure it to be more stand to attacks and vulnerabilities. This involves application updates and fixing security regularly, turning off unnecessary services or apps, applying for control access, applying the secure configuration, and applying system detection and prevention intrusion to the system.

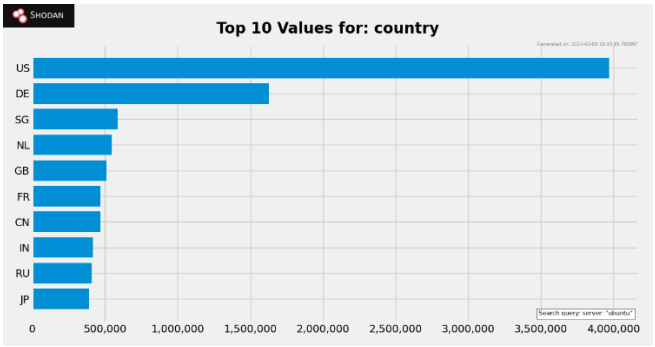
Shodan search engines (Bodenheim,et al., 2014) were used in a study to seek and estimate the use of a system operating Ubuntu server, i.e., system popular operation used as system server operation, which is used worldwide. The phrase following (1) is used as a search word to get how much data many Ubuntu servers exist and can recognize on the internet. Found

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

data showing that the United States (US), Germany (DE), Singapore (SG), Netherlands (NL), and United Kingdom (GB) are the top 5 countries with the most used system operating Ubuntu server and can recognize on the internet, the graphics can seen in Figure 1.

Figure 1.

User country for the Ubuntu Linux server operating system (Bodenheim et al, 2014).



The purpose of the study is to carry out the strengthening process security in a manner automatic for the system operating Ubuntu Linux, so strengthening security can apply in a manner immediately during the installation process system operation done with the help of application automation Hashicorp Packer. This solution allows doing a fully automated Ubuntu Linux installation process standard Ubuntu v1.1.0 CIS *benchmarks and* yields *Image* ready virtual machine used for production.

2. Discussion

Structure writing on papers served as follows. Draft baseline and review of the literature presented in Section 2. The proposed method is described in Section 3, where each development step is outlined in detail. Discussion and results from the proposed method are presented in Section 4, and conclusions are presented in Section 5.

Security Strengthening

Strengthening security is a secure process that reduces the possibility of an attack and minimizes possible vulnerabilities exploited by attackers (Ortiz-Garcés, 2021). Strengthening security system operation (OS) is strengthening specific security, focusing on security system operation, especially on the part operation and maintenance of the system operation. Then applying the proper configuration, deleting service or vulnerable apps, updating the device software, and setting rule security can help increase security system operation (OS), such as strengthening passwords and notes *login* user. Following *checklist* security that has set in a manner routine can do to be sure that policy security has done with Good is the most common technique used (Hamdani, 2021). One designated organization standard security on the system operation is the Center for Internet Security (CIS).

Ubuntu Servers

Ubuntu Linux is a free and open-source operating system based on the Linux kernel. This operating system was developed by Canonical Ltd., a software company based in the UK, and is one of the most popular Linux distributions available. Ubuntu has officially published three editions of Ubuntu Linux developed, namely: *Desktop, Server, and Core (for Internet of Things devices).*

Ubuntu 20.04 LTS was introduced on April 23, 2020; the latest version is 20.04.5, released on September 1, 2022. Support standard on version latest will end in April 2025 and end of life in April 2030. As LTS (Long et al.), this version of Ubuntu will get support for five

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

years, meaning users can rely on it to receive updated security and bug fixes for the long term. Ubuntu Server is considered a possible choice unreliable for the server environment because based on Debian, which has a reputation for being stable and safe. Ubuntu Server also includes several feature security, like AppArmor, which can help prevent access, and No legal and limited impact attacks.

Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a non-profit cybersecurity solutions provider founded in October 2000. CIS is focused on helping organizations improve their cybersecurity posture by providing best practices, tools, and resources (Aliyu et al, 2020). One of the most well-known resources provided by CIS is CIS Controls, which is a collection of 20 security control reference lists that organizations can use as a reference to improve their cyber security. CIS also provides various other resources, including benchmarks, assessments, and training programs. Organizational benchmarks guide organizations in securing specific systems and software, while the assessments help organizations identify areas of weakness in their cyber security defenses.

One of the CIS benchmark solutions designed by CIS is used to secure the Ubuntu 20.04 operating system. This benchmark provides several setting profiles. The level 1 profile is a basic guideline that can be adopted immediately and is made so that it does not significantly affect the system's performance. The Level 1 profile recommendations aim to reduce the likelihood of attacks on the organization while ensuring systems remain functional and usable without interruption.

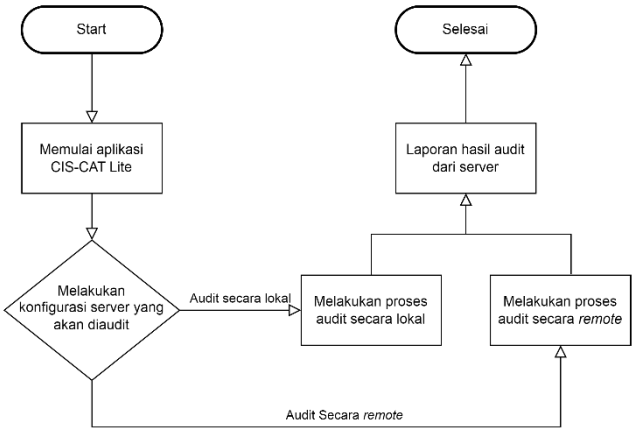
The Level 2 profile is designed as a more comprehensive approach to security and is intended for environments where protection is paramount. Recommendations regarding a Level 2 profile can significantly harm an organization if not implemented with care and rigor.

Center for Internet Security - Configuration Assessment Tool (CIS-CAT) Lite

The Center for Internet Security Configuration Assessment Tool Lite is a tool evaluation free made by CIS that helps users apply safe configurations for some technology by referencing standard security created by CIS. The CIS Configuration Assessment Tool scans the target system to search for vulnerabilities, identify weaknesses, and verify that the system complies with CIS standards. A higher score indicates a system that better complies with CIS criteria, thus making it more resistant to attack (Hamdani, 2021). The audit process uses the CIS-CAT Lite application can be depicted by the diagram flow in the image following Fig. 2

Figure 2

Flowchart of the audit process using the CIS-CAT Lite application



p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Packers

HashiCorp Packer is an application source possible open users to produce *Image* identical virtual machines for different platforms from one configuration source. This thing is possible user for produce *Images* consistently virtual machine for use in various scenarios, incl development, testing, and production. Kindly simple application. This allows standardization and automation, making *an Image* a virtual machine.

Packer uses an existing configuration file determined to make *an image* virtual machine with a launch virtual machine or container/entity while doing configuration and installation device required software, then wrap it up as *an Image* virtual machine for platforms that have been determined. *Image* generated virtual machine. Then can launch an entity new from the machine virtual with the device's same software and configuration precisely by a configuration defined on the packer app to ensure consistency throughout using the environment *Image* of the virtual machine.

Ansible

Ansible is a free and open-source app for managing infrastructure and applications system information [13]. Ansible allows you to automate configuration systems and applications, implementation systems, and administration throughout infrastructure users, whether on a physical server, virtual machine, or cloud-based resource. Ansible defines settings for target user server infrastructure in YAML files. The mutual organization of YAML files related to and used to perform automation configuration on the server is known as the Ansible playbook. This playbook includes a sequence of tasks describing the system's desired state and the procedures required to achieve that state. Ansible connects to the target system remotely via SSH or WinRM and runs mentioned task in playbooks.

Packer Server

Several stages are carried out in the research model, including the server packer installation process for solutions to automate and perform ESXi host configuration to support the smooth operation of the packer app alone. Make a server containing the Packer application and support to install the Packer app. Although the packer application can run almost every system surgery, in a research model, this chosen system operation is based on Ubuntu server 20.04 as the packer server to be used.

With reference from the source following, then made specification source power to use as packer server, as follows:

a) CPU: 2 Core Virtual CPU;
b) Memory: 4 Gigabytes;
c) Storage: 100 Giga bytes Virtual hard drive.

After preparing for the server to be used so furthermore is do install the packer application; following are the details of the application used:

a) Hashicorp packer version 1.6.0;
b) Ansible version 2.9.6;
c) VMware ovftool version 4.4.3 (build-18663434).

Furthermore, after preparing the packer server and configuring the ESXi host, the hypervisor version is ESXi version 5.5.0. Then done adjustment configuration on this host with several configurations as follows:

a) Enable SSH to ESXi Host.
b) Enable ESXi GuestIPHack.
c) ESXi firewall configuration for the VNC port

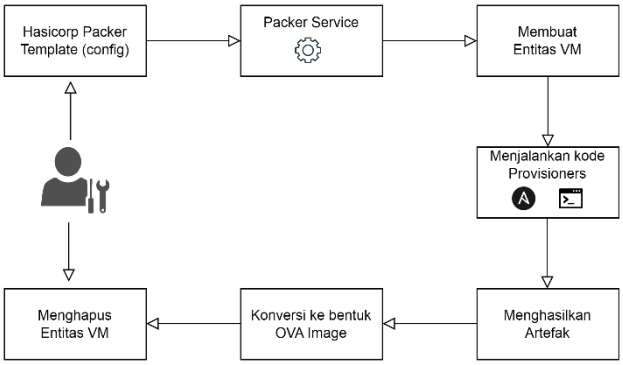
Lastly, the packer server is also a must. It can connect to the internet to update the repository and data transfer.

Figure 3

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Orginal Article

Packer application process flow



Then the process flow is carried out in the virtual machine image creation model using the application packer on research. This can be depicted in Figure 3. Process carried out: Make a template packer configuration. Next, the packer will make an entity virtual machine and will later do modifications for reinforcement security. Then reinforcement security is done automatically and controlled by the packer with equipment help like ansible and bash apps. After strengthening, so entity modified by control from CIS is ready to be converted into the OVA form. Entity previous virtual machine used will do deletion after the whole process is finished and produce results end in the form of a virtual machine image in OVA format.

User-data configuration

The user-data file is a script or can also be called a cloud-init file containing a command to do modification configuration and automation during installation in a cloud entity or running virtual machine system operation Ubuntu.

In the user-data configuration carried out in the study, this is to do configuration bullet points following during the automated installation process of the Ubuntu operating system use packer application:

a) Do identity configuration, such as the hostname, username, and password.
b) Do timezone configuration.
c) Do configuration allocation IP address.
d) Do partition layout configuration.
e) Do configuration for the SSH service, e.g., additional *ssh keys*.

This user-data file will later integrate with automation from the Packer using this user-data file; the usual process done the moment the installation from the installation media will automate and directly start the installation system operation without existing interaction from the user.

Ansible configuration based on CIS Benchmark

Ansible automation on research is used to do part excellent reinforcement process security by setting controls in CIS Ubuntu Linux 20.04 LTS Benchmark version 1.1.0. The whole process is packaged in the form of ansible playbook. Ansible playbook files Alone is a file in compiled YAML format in a manner order and run by defined inventory in ansible earlier. On research here, ansible-playbook arranged based on division controls that exist on the CIS Benchmark consists of 6 categories, namely:

a) Initial Setup;
b) Services;
c) Network Configuration;
d) Logging and Auditing;

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

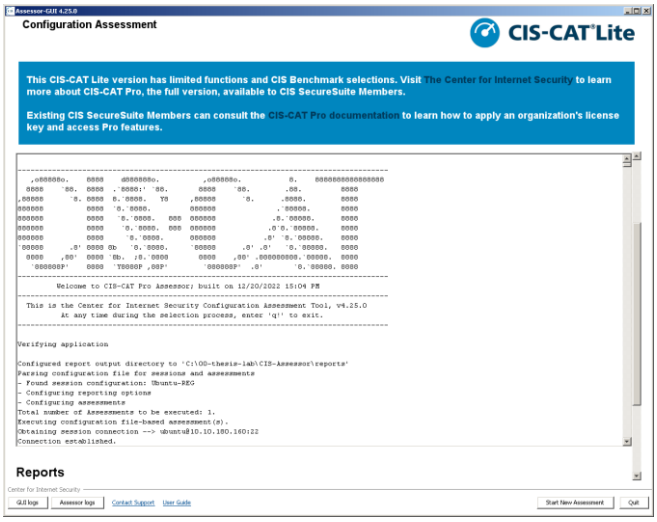
e) Access, Authentication, and Authorization;
f) System Maintenance.

Configuration *Ansible playbook* in study this, in a manner general, will direct operate CIS control for Server Level 2; however, If you want to use control specific or a different profile like Server -Level 1 can direct defined at the moment operate function on *Ansible playbook*.

Install the resulting VM Image and perform an audit assessment of the results of security strengthening

The resulting virtual machine image in the study uses the OVA format or *open virtual appliance*, i.e., the compressed file format of the OVF format, so generated one file for ease in its use and distribution. OVA format with easy can be used in almost all technology virtualization; on research, this is the OVA file that has been generated and will run on the environment virtualization Virtualbox. Furthermore, after running on the environment Virtualbox, verify that the control has been implemented in the research process. This has applied with the right, then audited from a virtual machine made from the resulting automation image. The tools used for conducting audits are CIS-CAT lite, a tool provided by CIS for conducting audits of benchmarks that have been approved. Published. View CIS-CAT applications can be seen in Figure 4.

Figure 4
CIS-CAT Lite application



The report generated by CIS-CAT Lite is an HTML file that can be seen with the help browser. Generated report enough comprehensive covers assessment per section control and summary whole the results obtained. As a measurement variable performed in research, This so used a comparison of two entities of the virtual machine; the first machine virtual used as reference is done Ubuntu virtual machine installation with following guidelines installation general in accordance step the guide that's on the Ubuntu installation media, next it is called standard ubuntu. Moreover, another uses the resulting OVA image from the study; next, it is called Ubuntu *hardened*.

Installed ubuntu virtual machine as standard ubuntu got results the audit score of CIS-CAT lite is 46.58% using server audit profile level 2, meaning Still There is a lack strengthening category safety *Initial setup, Network Configuration, Logging, and Auditing* as well as *Access, Authentication, and Authorization*. At the same time, the installed virtual machine as Ubuntu *hardened* to get the audit score of CIS-CAT Lite is 99.54%, where lack only is in the category *Logging and Auditing*. The results of data testing are attached in Table I. below.

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Orginal Article

Table 1
Cis-Cat Lite Audit Results on Test Entities

Test Entity	Test - Server Level 2			Score
	Passed	*Fail*	*Manuals*	
Standard Ubuntu	102	117	24	46.58%
Ubuntu Hardened	218	1	24	99.54%

With the use proposed methodology in a study, this is the implementation process of strengthening security with CIS Benchmark reference can standardize, especially on the system operating Ubuntu 20.04, so it can simplify the reinforcement process on the system operating Ubuntu 20.04 or If There is an update from the control that exists on CIS Benchmark can with easy applied. Furthermore, *image* virtual machines generated on research can speed up the development process of infrastructure technology information, particularly in critical environment-level security and compliance with standard safety (Padhy et al, 2021).

3. Conclusion

Packer application used is one solution automation for development infrastructure technology information, more from that application, this is also very helpful to do strengthening security to system the operation to be used in accordance standard general security. In research, this packer application collaborated with proven ansible can do automation security with standard CIS Benchmark security on the system operating Ubuntu 20.04 using profile server security – level 2, which is profile. This applies profile remember high security that can be applied to the system operation. Results achieved in research This can automate control on CIS benchmarks with conformity audit of 218 controls or 99.54% of the total 219 rules defined on CIS *Benchmark* for Ubuntu 20.04 version 1.1.0 using level 2 server profile. Ansible playbook used in research This can become a reference for developing CIS Benchmark standards for systems another operation because own ansible application can run on almost all existing system operations. Existing research methods can also be developed in the future, not limited to on-premise environments with virtualization ESXi just. However, it can also be used in a setting other than virtualization and on the environment *cloud*.

4. References

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

Hussain, S., Bahadur, F., Gul, F., Iqbal, A., Ashraf, G., & Nazeer, S. (2015). Survey of Windows and Linux as server operating system. *International Journal of Computer*, 18(1), 1-6.

Kleidermacher, D., & Kleidermacher, M. (2012). Embedded systems security: practical methods for safe and secure software and systems development. Elsevier.

Feller, J., & Fitzgerald, B. (2000). A framework analysis of the open source software development paradigm. In ICIS 2000 proceedings of the twenty-first international conference on information systems (pp. 58-69). *Association for Information Systems (AIS)*.

Chuyko, D. (2022). Best Linux distributions for server and cloud. https://bell-sw.com/announcements/2022/06/29/linux-distributions-for-server-and-cloud-overview/

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection, 7*(2), 114-123.

Ortiz-Garcés, I., Echeverría, A., & Andrade, R. O. (2021, July). Automation Tasks Model for Improving Hardening Levels on Campus Networks. *In 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)* (pp. 30-35). IEEE.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., ... & Khan, A. W. (2021). Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR), 54*(3), 1-36.