CyberSecurity and Digital Forensics
Vol. 5, No. 2, November 2022, p.83-88

e-ISSN: 2615-8442

SECURITY AUDITOR IMPLEMENTATION FOR STANDARDIZATION OF SERVER INSTALLATION ON SAAS SERVICES USING CIS BENCHMARK

Muhammad Najib[1], Bambang Purnomosidi[2], Muhammad Agung Nugroho[3]

[1]Informatika, Universitas Teknologi Digital Indonesia
Email: [1]175410171@students.akakom.ac.id, [2]bpdp@utdi.ac.id, [3]m.agung.n@utdi.ac.id

Abstract

The development of system services this year is increasing, especially SaaS services. In SaaS services, the need for information security is quite important. One of the solutions to improve security in the system is to harden the server used. Hardening can be done if you have configuration data on the design and controls for information security issues. This study aims to implement CIS Security to find out the results of an audit from CIS Benchmark in the form of an assessment so that it can improve the security of the Centos 6.10 operating system with recommendations from CIS Security. This research is building a system to conduct an audit on a server with the Centos 6.10 operating system; then, the audit results will be displayed in the data so that it is easier to read and can be used as material for evaluation for better SaaS service installations. In this security auditor system, there are two servers: a testing server and a pool server. Server testing is a server that will be audited using an audit program that is adjusted to the CIS Benchmark. This audit program is written in a bash script language. Audit results can be sent to the pool server and displayed by the pool server with a web page. This server pool uses PHP as the backend, with MySQL as data management. Audit results can be sent to the pool server and displayed by the pool server with a web page. This server pool uses PHP as the backend, with MySQL as data management. Audit results can be sent to the pool server and displayed by the pool server with a web page. This server pool uses PHP as the backend, with MySQL as data management.

At the same time, use the Bootstrap framework to beautify the front end. The server pool environment is run with docker virtualization. Based on the analysis, the results are a security auditor system for standardizing server installations in SaaS services using CIS Benchmarks. Building a security auditor requires standardization that has been recognized worldwide. CIS Control has an important link in the implementation of ISO 27001. The system can give a value to each audit result run on the testing server with CIS Benchmark based on CIS Control. In addition, this system provides a checklist of audit results data that System Administrators can use to evaluate server installations on SaaS services.

***Keywords**: network security auditing, CIS benchmark, CIS control, CIS security, ISO 27001*

1. INTRODUCTION

In the industrial era 4.0, the world's dependence on online services is getting higher. Thus the need for internet-based services is increasing. Along with the higher demand, traffic and services, cyber threats are also increasing. Threats(Yudha and Panji, 2018)it consists of Threats to service providers, which generally have threats on the server side such as SQL Injection, command injection, command execution, file inclusion, and server take over. Meanwhile, from the internet provider side, threats can be in the form of DDOS, smurfing, ARP poisoning, and BGP Attacking. Apart from threats to service providers, users are also threatened with security attacks such as client-side hacking, XSS, CSRF injection, viruses, trojans, etc.(Afif, 2017). In another approach, the attack can be in the form of social engineering where the methods used to obtain important information by deceiving the owner of the information, the mechanism can be done by telephone, internet applications, and other approaches such as using XSS techniques.

CIS Security is a method developed by CIS, whose mission is to identify, develop, validate, promote, and maintain the best solutions for cyber defense, building a societal mindset to improve a trusted environment in cyberspace. The method developed is the crowdsourcing model (involvement of other parties in the development of content and resources). CIS applies crowdsourcing in a closed manner (closed contribution). CIS Security(Sedano and Salman, 2021)has programs in environments such as CIS Control, CIS Benchmark, CIS Communities, and CIS Cybermarket.

In this study, the authors used objects in SaaS services developed by a technology and information company in Jogja. This SaaS is an academic system service for tertiary institutions with integrated compliance with DIKTI regulations. This system is known as E-campuz which manages the process of admission, registration, payment, academics, PDDikti reporting and student portals(Rozady, 2022). The use of this E-campuz system based on Cloud Computing with the SaaS model. The e-campuz service runs in the cloud, and the author will analyze the security of this service based on CIS benchmark implementation standards(Najib, 2021). The purpose of this study is to obtain security checklist data on SaaS services with CIS Control using CIS Benchmark, improve security in SaaS services by implementing CIS Control standardization from CIS Security, implementing ISO 27001 based on CIS, and control on SaaS services, and helping System Administrators in evaluating routine Saas service installations.

1.A. Information Security Management System

Information security in cyberspace or cybersecurity is technology, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.(Sari et al., 2020). Cyber security is also referred to as an effort to protect information from cyber attacks. Information Security Management System is a management system related to the implementation of information security in an organization which includes the activities of designing, implementing, and maintaining an integrated series of processes and systems to effectively manage information security, especially confidentiality, integrity, and availability of information assets while minimizing risk. that goes with it.

1.B. ISO 27001

ISO 27001 is a management system standard issued by ISO (International Organization for Standardization) in collaboration with IEC (International Electrotechnical Commission) which focuses on information security systems. This standard uses a control-based management approach based on risk analysis. This standard is widely applied, especially for companies/organizations that consider that information is a company asset that must be protected(February and Fitria, 2019). Furthermore, ISO/IEC 27001 is explained as one of the methods with information security standards issued by the International Organization for Standardization and the International Electrotechnical Commission. ISO 27001 is also defined as an information security management system standard document(Arini, 2019)or Information Security Management System, commonly called ISMS, which provides a general description of what an institution should do in their efforts to evaluate, implement, and maintain information security based on best practices in information security.

1.C. CIS Benchmarks

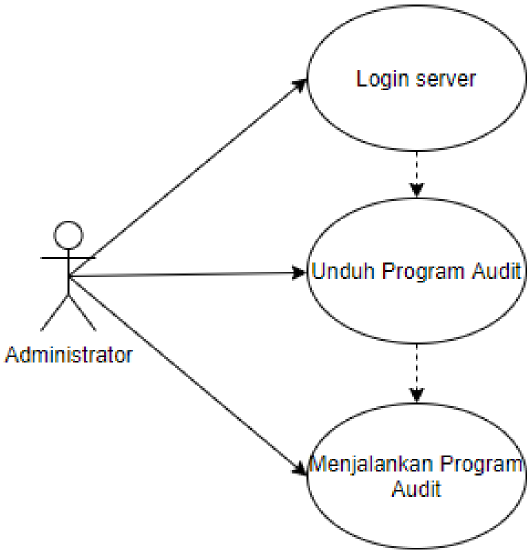
CIS Benchmarks are configuration baselines and best practices for configuring systems securely. Each guidance recommendation refers to one or more CIS Controls developed to help organizations enhance their cyber defense capabilities. CIS Control(cisecurity, 2022)maps to many defined standards and frameworksregulations, including the NIST Cyber Security Framework (CSF) and NIST SP 800-53, the ISO 27000 series of standards, PCI DSS, HIPAA, and others. It can also be interpreted as CIS Benchmark(Prastika et al., 2018)is a best-practice published by the Center for Internet Security (CIS) and documented for securely configuring IT systems, software, and networks. CIS Benchmarks are developed through a unique consensus-based process that engages a worldwide community of cybersecurity professionals and subject matter experts, each of whom is continuously identifying, refining, and validating security best practices within their area of focus.

2. METHODOLOGY

2.A. System Design

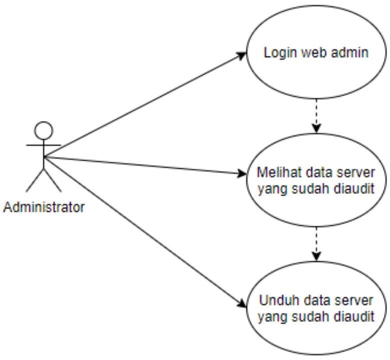
The process design in this study is explained in Figure 1. To run the audit program, starting from the administrator logging in to the server, then downloading the program first, then running the program on the server to be audited.

Figure 1. Use case diagram of running an audit program



Use Case Diagram for viewing and downloading audit results data is illustrated in Figure 2, namely when the administrator logs in to the web admin then the administrator can see which servers have been audited and the administrator can download audit results data from the server pool.

Figure 2. Use case diagram for viewing and downloading data


Login web admin
Administrator
Melihat data server yang sudah diaudit
Unduh data server yang sudah diaudit

Activity Diagram Audit process is described as having 3 parts, namely the administrator, system and server pool. The administrator is an actor. The three parts are interconnected starting from the administrator logging in as root to the system/server to be audited then downloading the audit program, then the next is running the audit program so that the system will process each audit simultaneously with the system displaying audited data on the monitor, then if the server has a connection, it will immediately send data to the server pool, otherwise an error message will appear on the screen. After the server pool gets data from the system being audited, the server pool will process the data into visual data and documents which can then be downloaded by the administrator.

*sequence*The diagram in the application made by the author is described in Figure 3, explaining the Admin flow when opening the all audit page. This happens when the Admin opens the all audit page the system will immediately validate whether the Admin is logged in or not, if not he will be redirected to the login page, if he is he will display the all audit page.

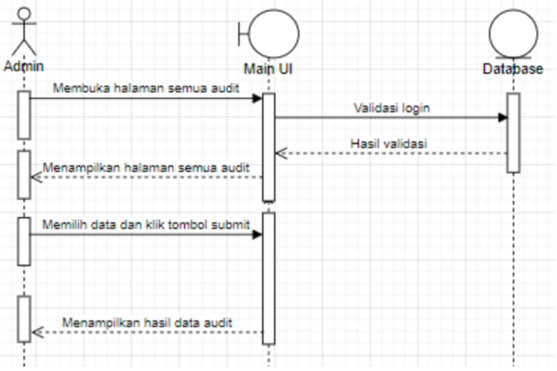
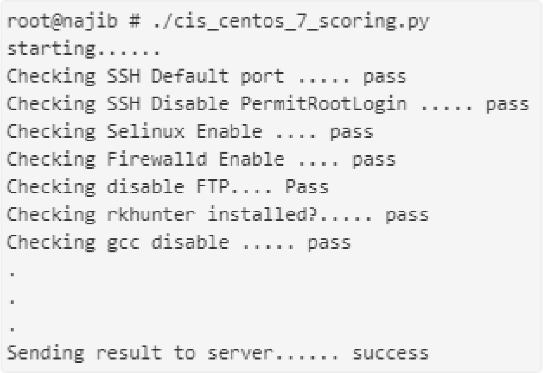

Admin
Main UI
Database
Membuka halaman semua audit
Validasi login
Hasil validasi
Menampilkan halaman semua audit
Memilih data dan klik tombol submit
Menampilkan hasil data audit

Figure 3. Sequence Diagram viewing all audit data

2.B. Interface Design

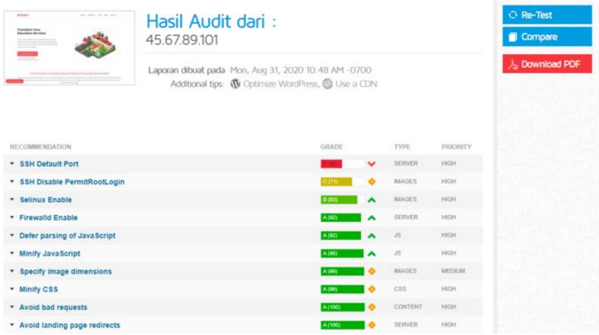
In this system the interface design is divided into two types, namely the interface design for the console base and also for the web base. Figure 4 describes the Console Base design which is the interface design when running an audit program based on CIS Benchmark. This audit program will be written in python. The monitor screen will display all data that has been audited and will appear on the monitor screen.



```
root@najib # ./cis_centos_7_scoring.py
starting......
Checking SSH Default port ..... pass
Checking SSH Disable PermitRootLogin ..... pass
Checking Selinux Enable .... pass
Checking Firewalld Enable .... pass
Checking disable FTP.... Pass
Checking rkhunter installed?..... pass
Checking gcc disable ..... pass
.
.
.
Sending result to server...... success
```

Figure 4. Console base interface design

The interface design in web form is illustrated in Figure 5. This page is for the dashboard display on a web browser, so on this page you can immediately see the audit results and also a button to download the audit results in PDF form.



Hasil Audit dari :
45.67.89.101

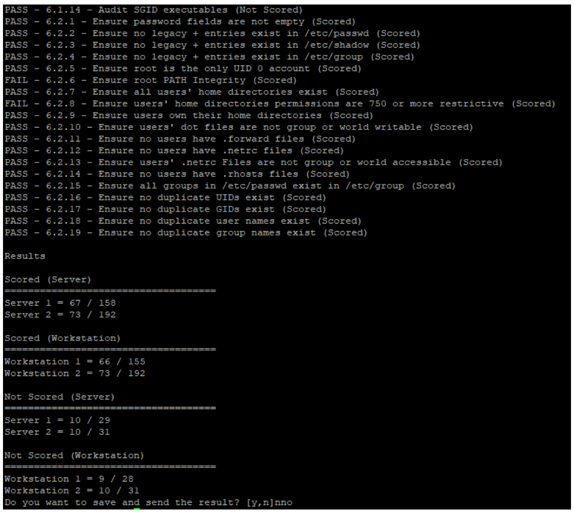
Laporan dibuat pada Mon, Aug 31, 2020 10:48 AM -0700
Additional tips: Optimize WordPress, Use a CDN

RECOMMENDATION	GRADE	TYPE	PRIORITY
SSH Default Port	[illegible]	SERVER	HIGH
SSH Disable PermitRootLogin	C (71)	IMAGES	HIGH
Selinux Enable	B (83)	IMAGES	HIGH
Firewalld Enable	A (92)	SERVER	HIGH
Defer parsing of JavaScript	A (92)	JS	HIGH
Minify JavaScript	A (96)	JS	HIGH
Specify image dimensions	A (99)	IMAGES	MEDIUM
Minify CSS	A (99)	CSS	HIGH
Avoid bad requests	A (100)	CONTENT	HIGH
Avoid landing page redirects	A (100)	SERVER	HIGH

Figure 5. Web base interface design

3. DISCUSSION

In this study the CIS Benchmark script was written using the bash programming language, in CIS_CentOS_Linux_7_Benchmark_v2.1.1 there are 223 points that are executed to document the configuration of an audited system as illustrated in the results of Figure 6.



```
PASS - 6.1.14 - Audit SGID executables (Not Scored)
PASS - 6.2.1 - Ensure password fields are not empty (Scored)
PASS - 6.2.2 - Ensure no legacy + entries exist in /etc/passwd (Scored)
PASS - 6.2.3 - Ensure no legacy + entries exist in /etc/shadow (Scored)
PASS - 6.2.4 - Ensure no legacy + entries exist in /etc/group (Scored)
PASS - 6.2.5 - Ensure root is the only UID 0 account (Scored)
FAIL - 6.2.6 - Ensure root PATH Integrity (Scored)
PASS - 6.2.7 - Ensure all users' home directories exist (Scored)
FAIL - 6.2.8 - Ensure users' home directories permissions are 750 or more restrictive (Scored)
PASS - 6.2.9 - Ensure users own their home directories (Scored)
PASS - 6.2.10 - Ensure users' dot files are not group or world writable (Scored)
PASS - 6.2.11 - Ensure no users have .forward files (Scored)
PASS - 6.2.12 - Ensure no users have .netrc files (Scored)
PASS - 6.2.13 - Ensure users' .netrc Files are not group or world accessible (Scored)
PASS - 6.2.14 - Ensure no users have .rhosts files (Scored)
PASS - 6.2.15 - Ensure all groups in /etc/passwd exist in /etc/group (Scored)
PASS - 6.2.16 - Ensure no duplicate UIDs exist (Scored)
PASS - 6.2.17 - Ensure no duplicate GIDs exist (Scored)
PASS - 6.2.18 - Ensure no duplicate user names exist (Scored)
PASS - 6.2.19 - Ensure no duplicate group names exist (Scored)

Results

Scored (Server)
====================================
Server 1 = 67 / 158
Server 2 = 73 / 192

Scored (Workstation)
====================================
Workstation 1 = 66 / 155
Workstation 2 = 73 / 192

Not Scored (Server)
====================================
Server 1 = 10 / 29
Server 2 = 10 / 31

Not Scored (Workstation)
====================================
Workstation 1 = 9 / 28
Workstation 2 = 10 / 31
Do you want to save and send the result? [y,n]nno
```

Figure 6. Display of audit results

After these points have been audited, an assessment will be carried out based on the Profile Definitions of the CIS Benchmark.

3.A. Assessment Information

The assessment status indicates whether compliance with the recommendations provided has an impact on assessing the benchmark score on the server being audited. The following is a benchmark of the status used:

1) *SCORED*, Failure to comply with the "SCORED" recommendations will lower the final benchmark score. Compliance with the "SCORED" recommendations will increase the final benchmark score.

2) *NOT SCORED*, Failure to comply with the "Not Scored" recommendations will not degrade the final benchmark score. Compliance with the "Not Scored" recommendation will not increase the final benchmark score.

3.B. *Profile Definitions*

*Profile Definitions*or the profile definition based on CIS is divided into 4, namely: Level 1 – Server, Level 2 – Server, Level 1 – Workstations and Level 2 – Workstations. Each profile has various characteristics and purposes, here are the complete definitions:

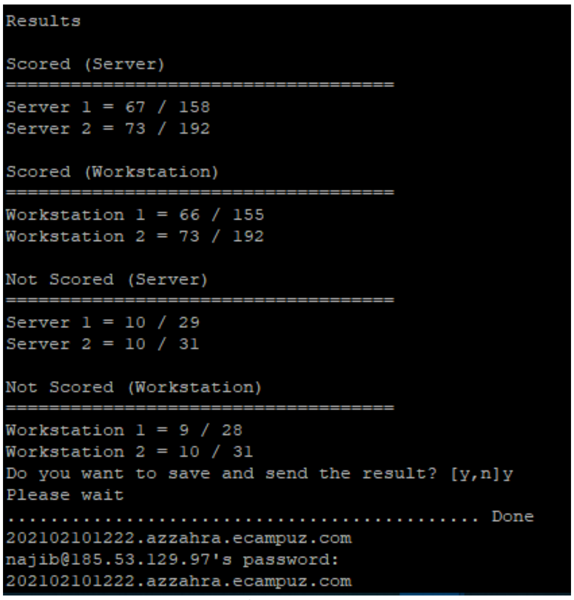
1) Level 1 – Server, Items in this profile are meant to be practical and discreet; Provides clear security benefits; and Does not inhibit the use of technology beyond acceptable capabilities.

2) Level 2 – Server, This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics: Intended for environments or use cases where safety is paramount; Acts as a defense in depth; May negatively hinder technology utility or performance.

3) Level 1 – Workstation, consists of Be practical and wise; Provides clear security benefits; and Does not inhibit the use of technology beyond acceptable capabilities.

4) Level 2 – Workstations, This profile extends the "Level 1 - Workstations" profile. Items in this profile exhibit one or more of the following characteristics : Intended for environments or use cases where safety is paramount; Acts as a defense in depth; May negatively hinder technology utility or performance.

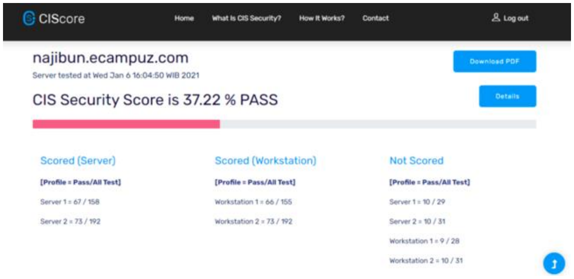
The developed system can carry out the process of storing audit results based on CIS benchmarks as shown in Figure 7.



```
Results

Scored (Server)
====================================
Server 1 = 67 / 158
Server 2 = 73 / 192

Scored (Workstation)
====================================
Workstation 1 = 66 / 155
Workstation 2 = 73 / 192

Not Scored (Server)
====================================
Server 1 = 10 / 29
Server 2 = 10 / 31

Not Scored (Workstation)
====================================
Workstation 1 = 9 / 28
Workstation 2 = 10 / 31
Do you want to save and send the result? [y,n]y
Please wait
............................................ Done
202102101222.azzahra.ecampuz.com
najib@185.53.129.97's password:
202102101222.azzahra.ecampuz.com
```

Figure 7. The process of storing and sending audit results

The results of system testing, scripts on the server can run and provide test results in the form of a CIS security score to be displayed from the front end. The CIS security score uses an assessment profile and profile definitions, the results of this system can be seen in Figure 8.



najibun.ecampuz.com
Server tested at Wed Jan 6 16:04:50 WIB 2021

CIS Security Score is 37.22 % PASS

Scored (Server)
[Profile = Pass/All Test]
Server 1 = 67 / 158
Server 2 = 73 / 192

Scored (Workstation)
[Profile = Pass/All Test]
Workstation 1 = 66 / 155
Workstation 2 = 73 / 192

Not Scored
[Profile = Pass/All Test]
Server 1 = 10 / 29
Server 2 = 10 / 31
Workstation 1 = 9 / 28
Workstation 2 = 10 / 31

Figure 8. Audit results

4. CONCLUSIONS AND RECOMMENDATIONS

Based on the research that was conducted during the Security Auditor Implementation for Server

Installation Standardization in SaaS Services Using CIS Benchmark, it can be concluded that system design requires recognized standardization related to information security management, one of which is the ISO 27001 standard. The system created adopts ISO 27001 using CIS Security To run CIS Control on a system requires the process of reading and documenting the configuration on a server. The process of reading and documenting configurations based on CIS Control based on CIS Benchmarks. The design of the security auditor system can run well and can be implemented with a script that is run to audit a Linux operating system, frontend and backend development using PHP.

Suggestions needed for the development of this system such as adding some audit scripts on operating systems other than Centos. Because currently the CIS Benchmark script only runs on the Centos operating system. Adding a module or feature that is used to add users to the application. Because at this time, adding users is still going through the database. Added a feature to filter audit results data to make it easier to search for data.

BIBLIOGRAPHY

AFIF, M.F., 2017. IMPLEMENTASI KEAMANAN OWASP TERHADAP APLIKASI BERBASIS GTFW (skripsi). STMIK AKAKOM Yogyakarta.

ARINI, A., 2019. PENDETEKSIAN DINI TINGKAT KEMANAN INFORMASI BERBASIS ISO 27001: 2013 MENGGUNAKAN METODE AHP (ANALYTICAL HIERARCHY PROCESS). Cyber Secur. Dan Forensik Digit. 2, 57–64.

CISECURITY, 2022. CIS Controls Version 8 [WWW Document]. Cent. Internet Secur. URL https://www.cisecurity.org/controls/v8/ (accessed 1.4.23).

FEBRUARI, P., FITRIA, F., 2019. Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung. POSITIF J. Sist. Dan Teknol. Inf. 5, 97–102. https://doi.org/10.31961/positif.v5i2.833

NAJIB, M., 2021. IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS ECAMPUZ MENGGUNAKAN CIS BENCHMARK (skripsi). STMIK AKAKOM YOGYAKARTA.

PRASTIKA, D.P., TRIYONO, J., LESTARI, U., 2018. AUDIT DAN IMPLEMENTASI CIS BENCHMARK PADA SISTEM OPERASI LINUX DEBIAN SERVER (STUDI KASUS: SERVER LABORATORIUM JARINGAN DAN KOMPUTER 6, INSTITUT SAINS & TEKNOLOGI AKPRIND YOGYAKARTA). J. Jarkom 6, 1–12.

ROZADY, M.P.N., 2022. TATA KELOLA TI DALAM PEMANFAATAN SISTEM E-CAMPUZ BERBASIS CLOUD COMPUTING PADA UNIVERSITAS NUSA NIPA MAUMERE. Increate - Inov. Dan Kreasi Dalam Teknol. Inf. 5.

SARI, I.Y., MUTTAQIN, M., JAMALUDIN, J., SIMARMATA, J., RAHMAN, M.A., ISKANDAR, A., PAKPAHAN, A.F., SUGIANTO, A.K., GIAP, Y.C., HAZRIANI, H., YENDRIANOF, D., MANULLANG, S.O., WATRIANTHOS, R., 2020. Keamanan Data dan Informasi. Yayasan Kita Menulis.

SEDANO, W.K., SALMAN, M., 2021. Auditing Linux Operating System with Center for Internet Security (CIS) Standard, in: 2021 International Conference on Information Technology (ICIT). Presented at the 2021 International Conference on Information Technology (ICIT), pp. 466–471. https://doi.org/10.1109/ICIT52682.2021.9491663

YUDHA, F., PANJI, A.M., 2018. PERANCANGAN APLIKASI PENGUJIAN CELAH KEAMANAN PADA APLIKASI BERBASIS WEB. Cyber Secur. Dan Forensik Digit. 1, 1–6. https://doi.org/10.14421/csecurity.2018.1.1.1216