IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111226

Intrusion Detection Prevention System Security Design With Encrypted Passwords and Secure Shell Crypto Keys

Sugiyatno[1], Mugiarso[2]

Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia[1]

Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia[2]

Abstract: Latar belakang penelitian, ini adalah penggunaan internet merupakan kebutuhan yang tidak dapat dihindari lagi. Dengan internet, segala sesuatu menjadi lebih mudah dan cepat. Namun dibalik kemudahan dan keuntungan dengan hadirnya internet, terdapat permasalahan yang menyertainya. Masalah keamanan telah menjadi fokus utama dalam dunia jaringan komputer, yang disebabkan tingginya ancaman yang mencurigakan (suspicious threat) dan serangan dari Internet. Keamanan Informasi merupakan salah satu kunci yang dapat mempengaruhi tingkat kehandalan (Reliability) suatu jaringan. Untuk mengatasi permasalahan keamanan jaringan dan komputer ada beberapa pendekatan yang dapat dilakukan. Salah satunya menggunakan sistem IDS (Intrution Detection System) dan IPS (Intrusion Prevention System). Tujuan penelitian ini adalah merancang sistem IDPS dengan password terenkripsi dan kunci kripto pada Secure Shell (SSH).

Keywords: Intrution Detection System; Intrusion Prevention System; Secure Shell.

I. INTRODUCTION

Intrusion Detection and Prevention System (IDPS) is a network security/threat prevention technology that examines network traffic flow to detect and prevent exploitation of vulnerabilities. Exploitation of a vulnerability is usually in the form of malicious input to a target application or service that an attacker uses to disrupt and gain control of the application [1]. After a successful exploitation, the attacker can disable the target application (resulting in a denial-of-service status), or potentially can access all rights and permissions available to the compromised application [2].

How many IDPS technology methodologies are used to detect attacks including signature-based, base anomalies, and stateful protocol analysis, etc. [3]. IDPS technology uses several methodologies, separately or integrated, to provide more extensive and accurate detection [4].

IDPS components can be connected through a network specifically designed for security software management known as network management. In network management, each sensor or agent host cannot pass other network traffic. The advantage of doing this is to hide the identity of the IDPS from attackers, protect the IDPS, and when adverse conditions such as worm attacks or denial of service are distributed on the network [5]).

Disadvantages of using network management include additional costs in network equipment and other hardware (eg PC for console) and administrators using separate computers for IDPS management and monitoring [6]

Encryption technique is one of the solutions to overcome the weaknesses in IDPS which still use additional devices. For encryption to work, both parties to the exchange must share the same key, and the key must be protected from access by others. Key changes to limit the amount of data compromised if an attacker learns the key.

Therefore, the strength of a cryptographic system rests on key distribution techniques, which refers to two parties wishing to exchange data, without allowing the other person to see the key [7]. In addition to encryption techniques, strong passwords that are frequently changed as well as encryption on passwords are required [8].

One of the encryption and decryption techniques is system text file data encryption with cryptography such as the Rivest Shamir Adleman (RSA) algorithm [9]. Algoritma RSA adalah algoritma asimetris teknik kriptografi yang memiliki dua kunci yaitu kunci publik dan kunci privat membuat proses deskripsi. Tujuan dari ini Penelitian ini merancang dan mengimplementasikan algoritma kriptografi RSA pada keamanan password user dan kunci kripto. Hasil

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111226

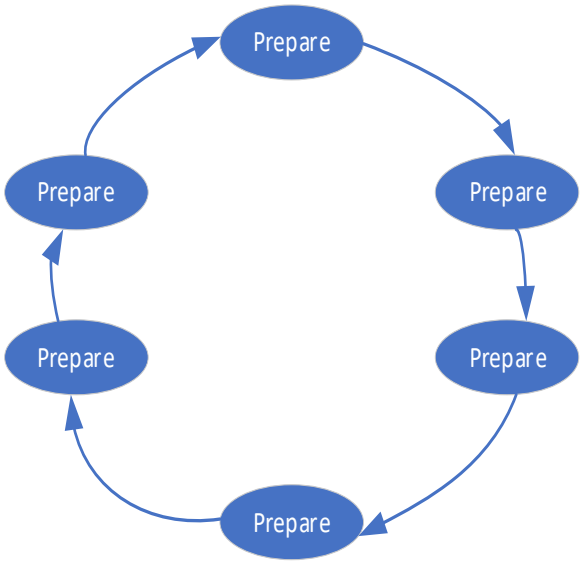
dari perancangan ini adalah sebuah konfigurasi pada router yang. diharapkan dapat diimplementasi pada infrastruktur yang akan digunakan [9]. In this research, we propose a bit-level encryption and decryption algorithm based on the number of keys that can encrypt 8-bit binary no to the corresponding 8-bit ciphertext and a decryption algorithm that can change the 8-bit cipher to 8-bit original text. The bit length can be extended to 16.32 bit binary numbers [10].

Intrusion detection systems greatly assist security administrators to secure networks, monitor and provide early warning. To manage an intrusion detection system is not simple and requires constant attention. The IDPS network must be positioned on the correct network and must be properly configured to send traffic to the IDPS [11].

II. RESEARCH METHODOLOGY AND LITERATURE SURVEY

Intrusion Detection and Prevention System (IDPS) design for network security with password encryption and crypto keys. With the Intrusion Detection and Prevention System (IDPS) you can filter incoming data such as email in the form of malware, spywares, Trojans which are reported every day.

In designing the IDPS using the PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) method) [12]. PPDIOO is a Cisco methodology used in computer network design that defines the continuous lifecycle of the services required for a computer network.



Gambar 1. Fase PPDIOO [12]

III. RESULT AND DISCUSSION

A. HARDWARE REQUIEMENTS SPECIFICATION

- 3 routers (Cisco 1941
- 2 switches (Cisco 2960 or comparable)
- 2 PCs (Windows Vista or Windows 7, TFTP server, Nmap/Zenmap, the latest version of Java, Internet
- Explorer, and Flash Player)
- Serial and Ethernet cables
- Console cables
- IPS Signature package and public crypto key files

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

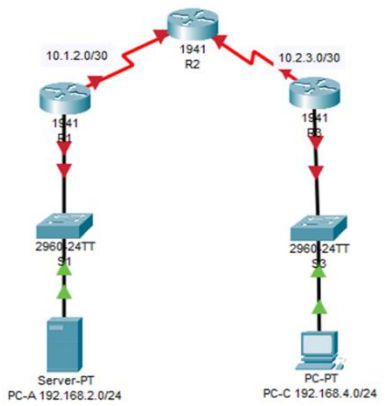
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

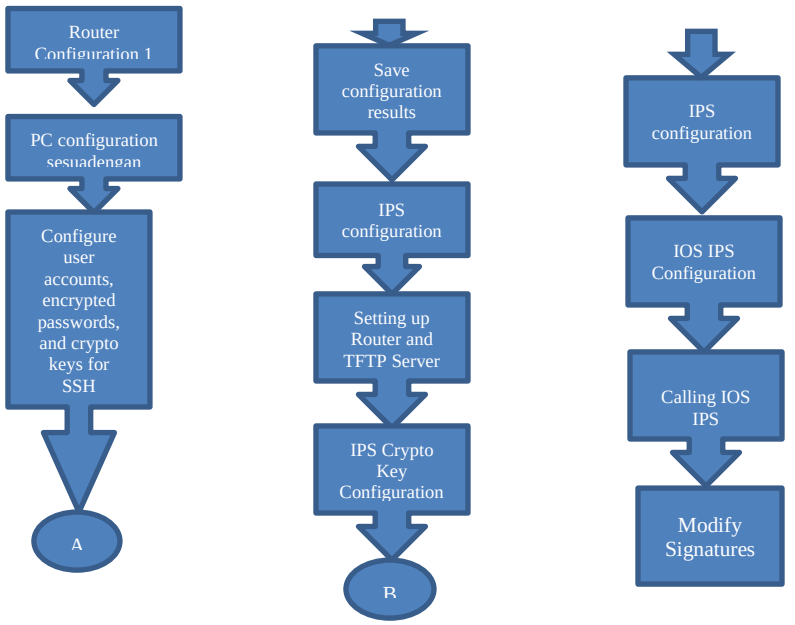
DOI: 10.17148/IJARCCE.2022.111226

B. DESIGN AND CONFIGURATION STAGE

1. Network Design



2. Configuration



C. TESTING STAGE

1. Test the number of compiled signature packages

```
R1# show ip ips signature count
Cisco SDF release version S364.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total
Signatures 11
   multi-string enabled signatures: 9
   multi-string retired signatures: 11

Signature Micro-Engine: service-http: Total
Signatures 662
   service-http enabled signatures: 163
   service-http retired signatures: 565
   service-http compiled signatures: 97
   service-http obsoleted signatures: 1

Signature Micro-Engine: string-tcp: Total
Signatures 1148
   string-tcp enabled signatures: 622
   string-tcp retired signatures: 1031
   string-tcp compiled signatures: 117
   string-tcp obsoleted signatures: 21

<Output Omitted>

Total Signatures: 2435
```

2. **Test the status of the IPS configuration status**

```
R1# show ip ips all
IPS Signature File Configuration Status
   Configured Config Locations: flash:ipsdir/
   Last signature default load time: 18:47:52 UTC Jan
6 2009
   Last signature delta load time: 20:11:35 UTC Jan 6
2009
   Last event action (SEAP) load time: -none

   General SEAP Config:
   Global Deny Timeout: 3600 seconds
   Global Overrides Status: Enabled
   Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
   Event notification through syslog is enabled
   Event notification through SDEE is enabled

IPS Signature Status
   Total Active Signatures: 339
   Total Inactive Signatures: 2096

IPS Packet Scanning and Interface Status
   IPS Rule Configuration
    IPS name iosips
```

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111226

Total Enabled Signatures: 1063 Total Retired Signatures: 2097 Total Compiled Signatures: 338 Total Obsoleted Signatures: 25 Jika ada pesan kesalahan selama kompilasi tanda tangan, seperti "%IPS-3-INVALID_DIGITAL_SIGNATURE: artinya Tanda Tangan Digital Tidak Valid (kunci tidak ditemukan)", berarti kunci kripto publik tidak valid	IPS fail closed is disabled IPS deny-action ips-interface is false Interface Configuration Interface Serial0/0/0 Inbound IPS rule is iosips Outgoing IPS rule is not set Interface FastEthernet0/1 Inbound IPS rule is iosips Outgoing IPS rule is not set IPS Category CLI Configuration: Category all: Retire: True Category ios_ips basic: Retire: False

D. ATTACK SIMULATION

Nmap/Zenmap is a network scanning tool that will find network hosts and resources, including services, ports, operating system, and other fingerprint information. Nmap should not be used to scan networks without prior permission. Because the act of scanning the network can be considered as a form of network attack. Nmap/Zenmap will test the IPS capabilities of the R1. By running the scan program from PC-A and trying to scan for open ports on router R2 before and after applying the iosips IPS rule on R1. The steps for starting the attack are as follows :

a. Download and install Nmap/Zenmap at http://nmap.org/download.html
b. Install Nmap/Zenmap.
c. Start Zenmap on PC-A
d. Masukkan IP address 10.1.1.2 pada Profile pilih Intense scan klik Scan

IV. CONCLUSION

With IPS enabled, the machine detects suspicious network traffic, can scan traffic, Network Administrators can create default and custom IPS policies to apply to IPS access rules can automatically accept intrusion prevention and update signatures periodically. And this design still needs development with other methods such as Contrail Service Orchestration (CSO).

ACKNOWLEDGMENT

The authors thank to Universitas Bhayangkara Jakarta Raya in supporting this research as internal research grant. Also, for the reviewers who have given the insightful comments.

REFERENCES

[1] J. Kizza and F. Migga Kizza, "Intrusion Detection and Prevention Systems," *Secur. Inf. Infrastruct.*, pp. 239–258, 2011, doi: 10.4018/978-1-59904-379-1.ch012.
[2] M. E. Kabay, "NIST's 'Guide to Intrusion Detection and Prevention (IDP) Systems," *Netw. World*, pp. 1–20, 2006, [Online]. Available: http://revistaie.ase.ro/content/65/12 - stanciu.pdf.
[3] A. Rahil, "The Challenges of Employee's Evaluation in Organizations," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 7, no. 2, pp. 33–45, 2017, doi: 10.6007/ijarbss/v7-i2/2614.
[4] I. C. L-, "Università degli Studi di Camerino Scuola di Scienze e Tecnologie IDS / IPS : Intrusion Detection / Prevention System Table of Contents," pp. 2012–2013, 2013.
[5] P. Baskerville, "Intrusion Prevention Systems: How do they prevent intrusion?," no. March, 2006, [Online]. Available: https://otago.ourarchive.ac.nz/handle/10523/1336.
[6] D. Kurniawan, Suparti, and Sugito, *Classification accuracy on the family planning participation status using kernel discriminant analysis*, vol. 1025, no. 1. 2018.
[7] D. Liestyowati, "Public Key Cryptography," *J. Phys. Conf. Ser.*, vol. 1477, no. 5, 2020, doi: 10.1088/1742-6596/1477/5/052062.
[8] E. Walkup, "The Password Problem," 2012, [Online]. Available: https://www.osti.gov/servlets/purl/1257179.
[9] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, "Design and Implementation of Rivest Shamir

DOI: 10.17148/IJARCCE.2022.111226

Adleman's (RSA) Cryptography Algorithm in Text File Data Security," *J. Phys. Conf. Ser.*, vol. 1641, no. 1, 2020, doi: 10.1088/1742-6596/1641/1/012042.

[10] S. Singha and M. Sen, "Encoding algorithm using bit level encryption and decryption technique," *2016 Int. Conf. Comput. Electr. Commun. Eng. ICCECE 2016*, vol. 160, no. 2, pp. 23–26, 2017, doi: 10.1109/ICCECE.2016.8009584.

[11] S. Ashoor, Asmaa Shaker., Gore, "Intrusion Detection System (IDS): Case Study Intrusion Detection System (IDS) & Intrusion Prevention System (IPS):," vol. 2, no. October, pp. 1–3, 2014.

[12] A. S. Elrashdi, S. E. Khiralla, and S. S. Albaseer, "Development PPDIOO methodology to be compatible with technical projects for computer networks," *Int. Sci. Technol. J.*, vol. 15, no. October, pp. 1–19, 2018, [Online]. Available: https://www.stc-rs.com.ly/istj/docs/volumes/Development1.pdf.

BIOGRAPHY

Sugiyatno has published some papers about Network and Security. She is now a lecturer of Informatics department in Universitas Bhayangkara Jakarta Raya.

Mugiarso Magister of Computer Science. He has been published papers in Data Mining, Machine Learning, and database. is still active as lecturer at Bhayangkara University.