Audit Configuration and Vulnerability Router on Diskominfos of Bali Province

Gede Ardi Herdiana[1], Made Sudarma[2]

[1]Department of Electrical and Computer Engineering, Post Graduate Program, Udayana University
[2]Department of Electrical and Computer Engineering, Udayana University

***Abstract*-Network security system on a computer that connected to the internet must be well planned and understood in order to effectively protect the resource in the network. how to find out the vulnerability of a network, so that by knowing the weaknesses in the network, then steps to overcome this drawback can be done. One of the forms taken includes conducting periodic analysis, both logical and physical. so that later it is expected that the analysis will produce an audit report containing the detection of various existing vulnerabilities, then take appropriate protective steps, which needed as a guarantee of security for the sustainability of the system. Nipper works by benchmarking the configuration of a router. After completing the inspection, you can see the configuration information as well as the security level of the router. Nessus works by scanning predetermined targets, such as a set of hosts or a separate host. Once the scan activity is complete, you can see the result information in either a graph or a line**

Index Terms - Vulnerability, Network Security, Nessus, Nipper

1. Introduction

The development of the world of telecommunications is currently very rapid along with the increasing need for fast and efficient services. Likewise, with data communication, from a connection between two computers to a computer network. Today's computer network is a service that is needed. Computer networks have more benefits than stand-alone computers. Computer networks allow sharing of data, software and equipment. So that the work group can communicate more effectively and efficiently [1].

Recently, personal identity theft through the internet has become increasingly common. Primarily, the targets are banking accounts along with bank account passwords and other important information. To prevent this, we need a network security system that aims to secure a system so that the data in the system is not used by other people.

A computer network security system connected to the Internet must be well planned and understood in order to effectively protect the resources in the network. A secure system (secure system) is assumed to be a system in which an intruder must sacrifice a lot of time, effort, and undesirable costs in the framework of the attack, or the risk that must be incurred is not worth the benefits that will be obtained.

2. Literature Review

2.1 Audit

Business organization undergo different types of audits for different purposes. The most common of These are external (financial) audits, internal audits, and fraud audits. An IT audit focuses on the computer-based aspects of an organization's information systems and modern systems employ significant levels of technology [2]. Audit is playing an important role in developing and enhancing the global economy and business firms [3]. Ron Weber (1999) argued, that Information systems auditing is the process of collecting and evaluating evidence to determine computer system safeguard asses, maintain data integrity, allow organizational goals to be achieved effectively, and use resources efficiently [4]. According Sukrisno Agoes (2004), "An examination conducted critically and systematically by an independent party, the financial statements have been prepared by management along with notes bookkeeping and supporting evidence, in order to be able to give an opinion on the fairness of the financial statements" [5].

2.2 TCP/IP (Transmission Control Protocol/Internet Protocol)

Protocol is a rule that being applied in data communication process which its process is identified based on its service type. Each protocol running will be named according to the process conducted in communication process of computer network [6].

Transmission Control Protocol/Internet Protocol (TCP/IP) is a protocol for sending data between computers on a network. This protocol is a protocol used for internet access and is used for global communications. TCP/IP consists of two separate protocols. TCP / IP used a layer approach when building this protocol. This layered approach allows the construction of several small services for specific tasks. TCP / IP consists of five layers [7]:

A. Application Layer
Within this layer applications such as FTP, Telnet, SMTP, and NFS are implemented.

B. Transport Layer
Within this layer TCP and UDP add transport data to the packet and pass it to the Internet layer.

C. Internet Layer
This layer takes packets from the transport layer and adds address information before sending them to the network interface layer.

D. Network Interface Layer
In this layer data is sent to the physical layer via network devices.

E. Physical Layer
This layer is a cable system used for the process of sending and receiving data.

2.3 Local Area Network

Local Area Network (LAN) is a privately owned network in a building or campus measuring up to several kilometers with a destination share resources and exchange information [8]. LAN was created to save costs in the use of tools together, but over time the functions increase. A communication channels can be shared by many computers which are connected to one another. Channel sharing communication is the main key in the efficiency of computer networks become a very large network like the Internet [9].

2.4 Understanding Computer Networks

A computer network is a collection of computers and their mechanisms and procedures which are connected and communicate with each other. Communication carried out by computers it can be the transfer of various data, instructions, and information from one computer to other computers [10].

2.5 Network Security Concept

Network security issues are very important and deserve attention. Networks connected to the internet are inherently insecure and can always be exploited by hackers, both LAN and wireless networks. When data is sent, it will pass through several terminals to arrive destination, that's means that it will provide an opportunity for other users who are not responsible to intercept or modify the data. In developing its design, a network security system connected to the Internet must be well planned and understood in order to protect the resources within the network effectively and minimize attacks by hackers. If you want to secure a network, you must first determine the level of threats that must be overcome, and the risks that must be taken or which must be avoided. The following will discuss threats, weaknesses, and network security policies [1].

2.6 Security Policy

security policy is a set of rules that determine what is allowed and what is prohibited from the use or utilization of access to a system during normal operation. Establishment of a security policy should be written in detail and clearly. The duties and determination of the security policy are usually political decisions of the company management [11]. Threat analysis is an audit process in which all possible attacks against the system are carefully identified. A record listing all possible abuse and disruptions to the system should be kept as a basis for warning.

The application of security policy rules should be carried out systematically by first carrying out an initial analysis, be it an analysis of physical or logical installations, including: auditing and balancing the costs of system protection with the risks that arise, then implementing the mechanism - The security mechanism that has been designed, for example, is an access control mechanism that explains which objects are allowed to be accessed by the public and which are not [12].

2.7 Basic Definition of Vulnerability

A vulnerability is a point of weakness where a system is vulnerable to attacks. A threat (threats) is a thing that is dangerous for the sustainability of the system. There are three key words that arise and are related to each other when we discuss the issues of computer security, namely: vulnerabilities, threats, and countermeasures. The danger can be a human (a system cracker or a spy), a damaged equipment, or an event such as fire and flood, which may exploit the vulnerability of a system. The more vulnerabilities and threats that can occur in a system, the higher our awareness should be to be able to protect the system and information in it. A technique for protecting a system is called a precautionary measure (countermeasures) [13].

2.8 Nipper Studio

Nipper Studio performs analysis of firewalls, routers, switches and other network devices. Paws Studio performs analysis of servers, workstations, laptops, enterprise applications and systems running Windows, Linux or Mac OS. Both tools are certified as 100% accurate and can be used onsite, online, offline, in the cloud, virtually or integrated into an enterprise system [14].

Nipper quickly identifies undiscovered vulnerabilities in firewalls, switches and routers, automatically prioritizing risks to your organization. Our virtual modelling reduces false positives and identifies exact fixes to help you stay secure and compliant [15].

2.9 Nessus

Nessus works by checking targets that you have defined, such as a set of hosts or it could be hosts in a separate focus. Once the scan activity is complete, you can see the result information in either graphical or line form. Nessus graphical interface was built using the Gimp Toolkit (gtk) [7]. Tenable Network Security, Inc. is a group of organizations authorized to write and build the Nessus Security Scanner application. And consistently this organization continues to develop this application. Tenable in this case writes almost all plugin facilities that are currently available, such as specifically to help Scanner activity according to broader audit needs and policies. [12].

3. DISCUSSIONS

3.1 Nipper Benchmark Result

Nipper performed a Security Audit of Router on Diskominfos of Provinsi Bali Office and identified 19 security-related issues. Nipper can draw the following statistics from the results of the security assessment. 3 issues (16%) were rated as high, 5 issues (26%) were rated as medium, 9 issues (47%) were rated as low and 2 issues (11%) were rated as informational. Here the result and the recommendation from Nipper.

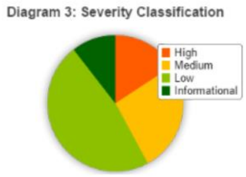


Diagram 3: Severity Classification

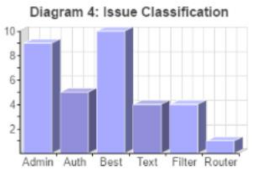
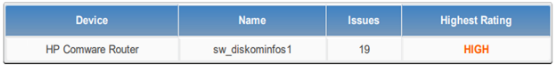
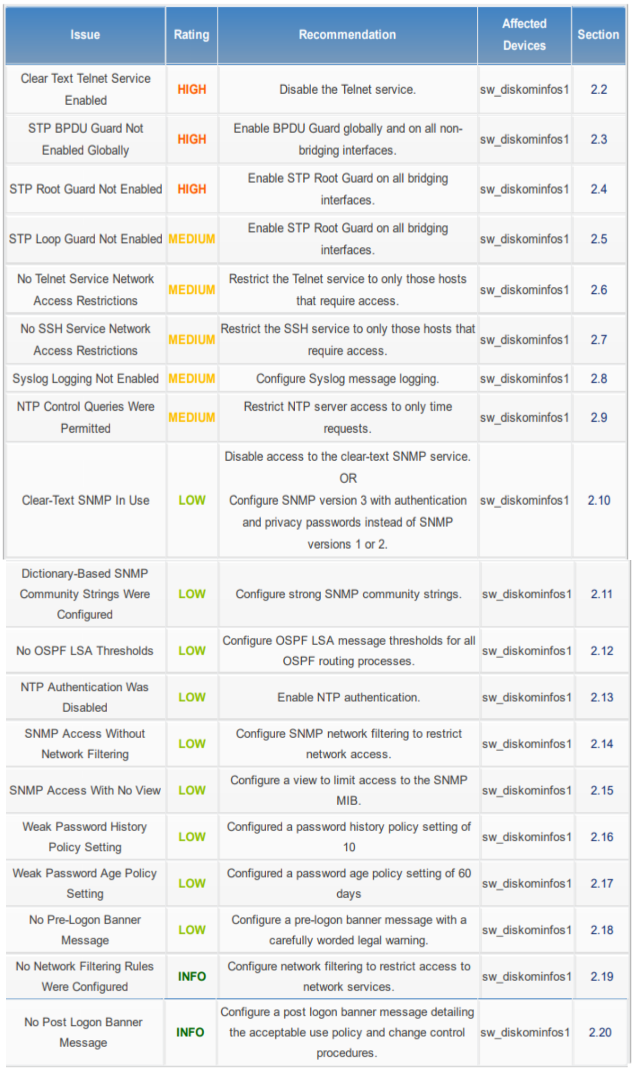


Diagram 4: Issue Classification



Device	Name	Issues	Highest Rating
HP Comware Router	sw_diskominfos1	19	HIGH



Issue	Rating	Recommendation	Affected Devices	Section
Clear Text Telnet Service Enabled	HIGH	Disable the Telnet service.	sw_diskominfos1	2.2
STP BPDU Guard Not Enabled Globally	HIGH	Enable BPDU Guard globally and on all non-bridging interfaces.	sw_diskominfos1	2.3
STP Root Guard Not Enabled	HIGH	Enable STP Root Guard on all bridging interfaces.	sw_diskominfos1	2.4
STP Loop Guard Not Enabled	MEDIUM	Enable STP Root Guard on all bridging interfaces.	sw_diskominfos1	2.5
No Telnet Service Network Access Restrictions	MEDIUM	Restrict the Telnet service to only those hosts that require access.	sw_diskominfos1	2.6
No SSH Service Network Access Restrictions	MEDIUM	Restrict the SSH service to only those hosts that require access.	sw_diskominfos1	2.7
Syslog Logging Not Enabled	MEDIUM	Configure Syslog message logging.	sw_diskominfos1	2.8
NTP Control Queries Were Permitted	MEDIUM	Restrict NTP server access to only time requests.	sw_diskominfos1	2.9
Clear-Text SNMP In Use	LOW	Disable access to the clear-text SNMP service. OR Configure SNMP version 3 with authentication and privacy passwords instead of SNMP versions 1 or 2.	sw_diskominfos1	2.10
Dictionary-Based SNMP Community Strings Were Configured	LOW	Configure strong SNMP community strings.	sw_diskominfos1	2.11
No OSPF LSA Thresholds	LOW	Configure OSPF LSA message thresholds for all OSPF routing processes.	sw_diskominfos1	2.12
NTP Authentication Was Disabled	LOW	Enable NTP authentication.	sw_diskominfos1	2.13
SNMP Access Without Network Filtering	LOW	Configure SNMP network filtering to restrict network access.	sw_diskominfos1	2.14
SNMP Access With No View	LOW	Configure a view to limit access to the SNMP MIB.	sw_diskominfos1	2.15
Weak Password History Policy Setting	LOW	Configured a password history policy setting of 10	sw_diskominfos1	2.16
Weak Password Age Policy Setting	LOW	Configured a password age policy setting of 60 days	sw_diskominfos1	2.17
No Pre-Logon Banner Message	LOW	Configure a pre-logon banner message with a carefully worded legal warning.	sw_diskominfos1	2.18
No Network Filtering Rules Were Configured	INFO	Configure network filtering to restrict access to network services.	sw_diskominfos1	2.19
No Post Logon Banner Message	INFO	Configure a post logon banner message detailing the acceptable use policy and change control procedures.	sw_diskominfos1	2.20

Nipper identified three HIGH rated security issues. Nipper determined that:

- The Telnet service was enabled
- BPDU Guard was not enabled globally
- STP Root Guard was not enabled on all bridging interfaces

Nipper identified five medium rated security issues. Nipper determined that:

- STP Root Guard was not enabled on all bridging interfaces
- No Telnet network host access addresses were configured
- No SSH network host access addresses were configured
- The logging of system message to a Syslog logging server was not configured
- NTP control queries were permitted

Nipper identified nine LOW rated security issues. Nipper determined that:

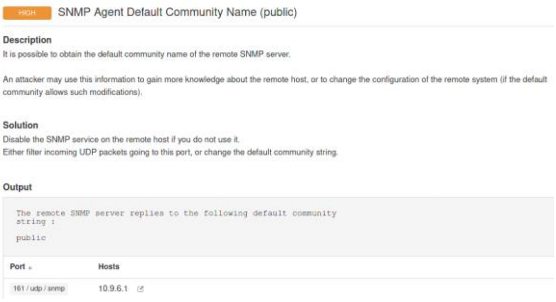
- the clear-text SNMP service was enabled
- dictionary-based SNMP community strings were configured
- no OSPF LSA message thresholds were co nfigured
- NTP authentication was disabled
- network filtering was not configured to rest rict SNMP access
- SNMP community strings were configured without a view
- a weak password history policy setting was configured
- a weak password age policy setting was co nfigured
- no pre-logon banner message was configur ed

Nipper identified two INFO rated security issues. Nipper determined that:

- no network filtering rules were configured
- no post logon banner message was configur ed

3.2 Nessus Scanner Results

Nessus Performed a vulnerability scanner of Router on Diskominfos of Provinsi Bali host. Scanning is done to find out if a host in a computer network has a vulnerability or does not depend on the security of each host. The following is a scan of hosts with no vulnerability and hosts with vulnerabilities.



HIGH SNMP Agent Default Community Name (public)

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

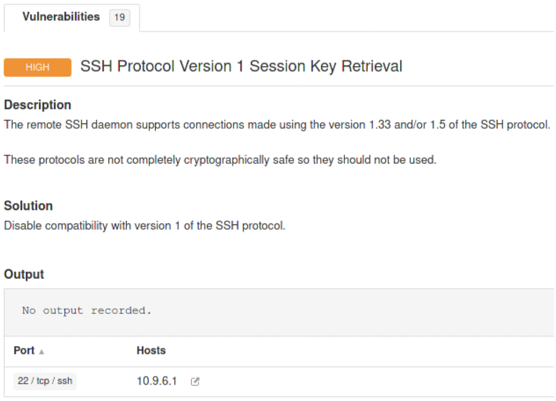
Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Output

```
The remote SNMP server replies to the following default community
string :

public
```

Port ▲	Hosts
161 / udp / snmp	10.9.6.1



Vulnerabilities 19

HIGH SSH Protocol Version 1 Session Key Retrieval

Description

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

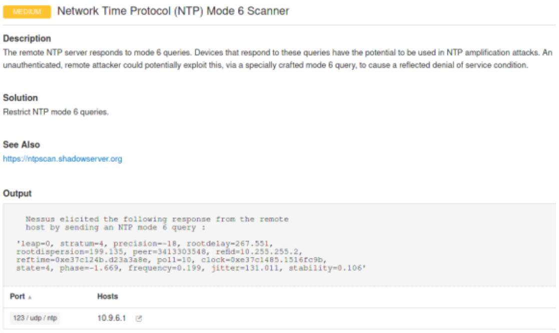
Solution

Disable compatibility with version 1 of the SSH protocol.

Output

```
No output recorded.
```

Port ▲	Hosts
22 / tcp / ssh	10.9.6.1



MEDIUM Network Time Protocol (NTP) Mode 6 Scanner

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

Solution

Restrict NTP mode 6 queries.

See Also

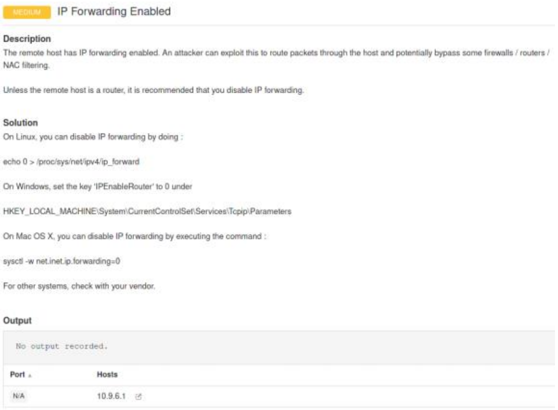
https://ntpscan.shadowserver.org

Output

```
  Nessus elicited the following response from the remote
  host by sending an NTP mode 6 query :

'leap=0, stratum=4, precision=-18, rootdelay=267.551,
rootdispersion=199.135, peer=3413303548, refid=10.255.255.2,
reftime=0xe37c124b.d23a3a8e, poll=10, clock=0xe37c1485.1516fc9b,
state=4, phase=-1.669, frequency=0.199, jitter=131.011, stability=0.106'
```

Port ▲	Hosts
123 / udp / ntp	10.9.6.1



MEDIUM IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Output

```
No output recorded.
```

Port ▲	Hosts
N/A	10.9.6.1

Scanning result on host 10.9.6.1

- SNMP Agent Default Community Name (public)
- SSH Protocol Version 1 Session Key Retrieval
- Network Time Protocol (NTP) Mode 6 Scanner
- IP Forwarding Enabled

4 Conclusions

- Internet computer networks that are public and global in nature are basically less secure and to increase the security of the internet network, several methods can be used, for example, authentication methods, use of encryption-decryption methods, and using a firewall.
- Weaknesses of a network system can be seen using tools such as scanners, TCP / IP assemblers, Network Protocol Analyzer, and others.
- Several vulnerability problems in the Router on Diskominfos of Bali Province, such as the Telnet service, are intentionally enabled because this feature is used to perform Remote Login, making it easier for employees to perform maintenance.

- Nessus and Nipper can be used to find out the weaknesses of the network and also generate information, conditions and solutions to the weaknesses experienced by the host.

REFERENCES

[1] b. a. nugroho, "Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan packet Sniffing," 2012.

[2] J. Hall, "Information Technology Auditing and Assurance" Third Edition, South-Western: Cengage Learning, 2011.

[3] H. A. Khaddash, R. A. Nawas, A. Ramadan, "Factors Affecting the quality of Auditing: The Case of Jordanian Comercial Banks," *International Journal of Business and Social Science,* vol. 4 no 11, pp. 206-222, 2013.

[4] E. Maria, E. Haryani, "Audit Model Development of Academic Information System : Case Study on Academic Information System of Satya Wacana," *International Refereed Research Journal* , vol. II, no. 2, pp. 12-24, 2011.

[5] Komang Budiarta, Adi Panca Saputra Iskandar, Made Sudarma, "Audit Information System Development using COBIT 5 Framework," *International Journal of Engineering and Emerging Technology* , vol. 1 No 1, 2016.

[6] Made Sudarma, Dandy Pratama Hostiadi, "The Establishment of Decision Tree Model in Network Traffic Incident Using C4.5 Method," *International Journal of Informatics and Communication Technology (IJ-ICT),* vol. 3, pp. 23-29, 2014.

[7] D. Juardi, "Kajian Vulberability Keamanan Jaringan Internet Menggunakan Nessus," pp. 11-19, 2017.

[8] T. A. S., Jaringan Komputer, Edisi Bahasa Indonesia, Edisi III, Jakarta: Prenhallindo, 1996.

[9] I. Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik," *JUSI,* vol. 1 No 1, 2001.

[10] R. Arief, Student Guides Series Pengenalan Jaringan Komputer, Jakarta: PT Elex Media Komputindo, 2006.

[11] R. Rahmat, Panduan Membangun Jaringan Komputer untuk Pemula, jakarta: PT Elex Media Komputindo, 2003.

[12] Z. Amin, "Analisis Vulnerabilitas Host pada Keamanan Jaringan Komputer di PT Sumeks Tivi Palembang (PALTV) Menggunakan Router Berbasis Unix," *Jurnal Teknologi dan Informatika (TEKNOMATIKA),* vol. 2, pp. 189-199, 2012.

[13] Gangemi, Lehtinen, Russell, Computer Security Basics, United Stated of America: O'Reilly Media, 2009.

[14] T. Ltd, "Linkedin," Computer Software, [Online]. Available: https://www.linkedin.com/company/titania-ltd. [Accessed 20 12 2020].

[15] T. Nipper, "Linkedin," Computer & Network Security, [Online]. Available: https://www.linkedin.com/showcase/nipper-studio?trk=affiliated-pages_result-card_full-click. [Accessed 20 12 2020].