ATCS System Security Audit Using Nessus

Sri Ariyani Arta Wijaya
Department of Electrical and Computer Engineering, Faculty of Engineering, Udayana University

The research is financed by personal academic research

Abstract

Threats to a web abstraction is likely to occur and it is difficult to say that the web will be safe and free of threats or attacks from the attacker. a web which is connected to the computer network will be accessible to all parties so that there is always a lurking threat. To minimize the threat of a web in advance in the evaluation before it is published to a web server. How the analysis of the web that is by looking for weaknesses that could be the entrance to an attacker control of the web. The term is often used in analyzing the weaknesses that the analysis of vulnerability scan web application using Nessus. On the client side is Nessus will be installed and running to find out the weaknesses that exist. From the research that has been done that the web is analyzed contained one drawback with the category of medium and info. Within these categories can be known weaknesses and solutions to address in detail so that weaknesses can be minimized before the web uploaded on the web server.

Keywords: Nessus, Vulnerability, Network Security, Audit Report, Penetration Test

1. INTRODUCTION

Network security is one of the fundamental things that repenting and in the utilization of a system. A weakness in a computer network system is often disregarded, until the event of a threat or a destructive attack on the system, the impact will be worse and very harmful. Consideration of the dangers and disadvantages of misuse of services on the local network and all Internet-based applications today, then it should businesses and organizations to implement a strategy of initial steps to mitigate them. One way in which of them is to do an analysis on a periodic basis, both logic and physics, so that might be expected from the analysis produces a report that shows the detection of weaknesses of the various vulnerabilities that exist, to then take the steps appropriate protection, which is required as a security guarantee for the sustainability of the system [1].

2. LITERATURE REVIEW

2.1 ATCS

Area Traffic Control System or better known as the ATCS is a traffic control system based on information technology in an area that aims to optimize the performance of the road network through optimization and coordination arrangements traffic lights at every intersection. ATCS consists of several main systems [2]:

1. Server, Workstation, which serves as the operations center to monitor and control the traffic conditions of the entire intersection in one area.
2. Wall map, which serve to provide information on the status and conditions of the Local Controller.
3. Local Controller (controller intersection).
4. Video Surveilance (CCTV).
5. Vehicle Detector.

2.1.1 Functions ATCS

1. Set the time signal at the intersection of the responsive and coordinated.
2. Under certain circumstances, give a green vehicle that has priority (Fighting Vehicle, Ambulance, VVIP, Convoy, etc.)
3. Delivering information on traffic conditions and alternate tracks.
4. Provides recorded traffic data, the incidence of accidents, and other events at the junction[2].

2.1.2 Benefits ATCS

1. The creation of a road network performance optimization.
2. Realizing the traffic system and road transport that is secure, safe and environment.
3. Reducing the number and burden of traffic control officers at the junction [2].

2.2 Vulnerability Scanner

Vulnerability scanner is a comput er program designed to locate and map the system for weaknesses in the application, computer or network. The increasing use of the internet to make more and more websites are popping up. But it is unfortunate Internet crimes continue to increase as the emergence of diverse articles that discusses hacking issues [3]. applications used to analyze the weaknesses of the system is Nessus. Nessus is a free scanner. Nessus is distributed under the GNU Public License from the Free Software Foundation.

2.3 Nessus

Nessus is a remote security scanning tool that is used to automatically perform testing on security issues, in particular to find vulnerabilities that an attacker can gain access to a host that is connected in a network [3].

2.3.1 How it work of Nessus

Nessus perform scanning based Security Policy Plugin that we activate (enabled) before scanning. Security Policy itself is a set of rules that defines the things what is allowed and what is forbidden to use or utilization of access on a system during normal operation. Example eg, Nessus can know which ports are open on a computer connected to a network such as the Internet. By knowing which ports are open, we can find out the possible cause of damage or knowing whichever path it is possible to access our computers. There are four parts in the configuration menu Policies, which are: General, Credentials, Plugins and Preferences. The explanation of the parts of the above configuration is [1]:

1. General serves to provide a naming policy (policy) and provide some techniques for configuring the scan is in progress.
2. On the Credentials tab, we can add security configuration such as authentication, key words or password on the SMB protocol (service messages block), domain name, keywords SSH protocol throughout the scanning process, by providing configuration on the Credentials tab, we'll get the results of scanning and inspection more accurate and diverse.
3. On the Options tab plugin users, can select specific types needed plugin, this plugin menu choice will assist you in categorizing the types of attacks, and the vulnerability is often the case today, be it against the service that is being run, ports which should not be opened, an operating system vulnerabilities, bugs or security holes in certain instruments, platforms and types of the most current virus variants.

3. RESEARCH METHOD

The method used in the analysis of vulnerability scan the web in a way ATCS using Nessus App. Web that will be scanned are ATCS Denpasar with public IP is 202.51.199.246.

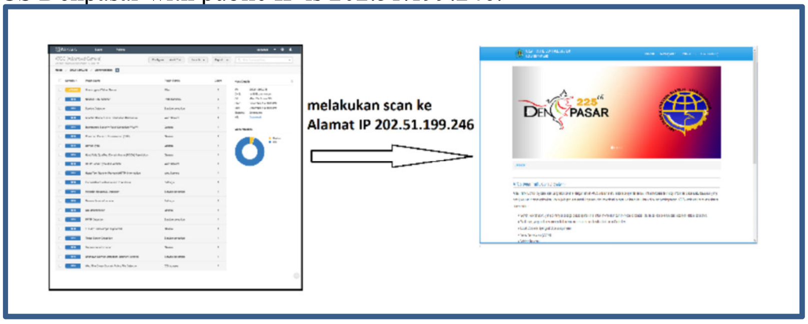
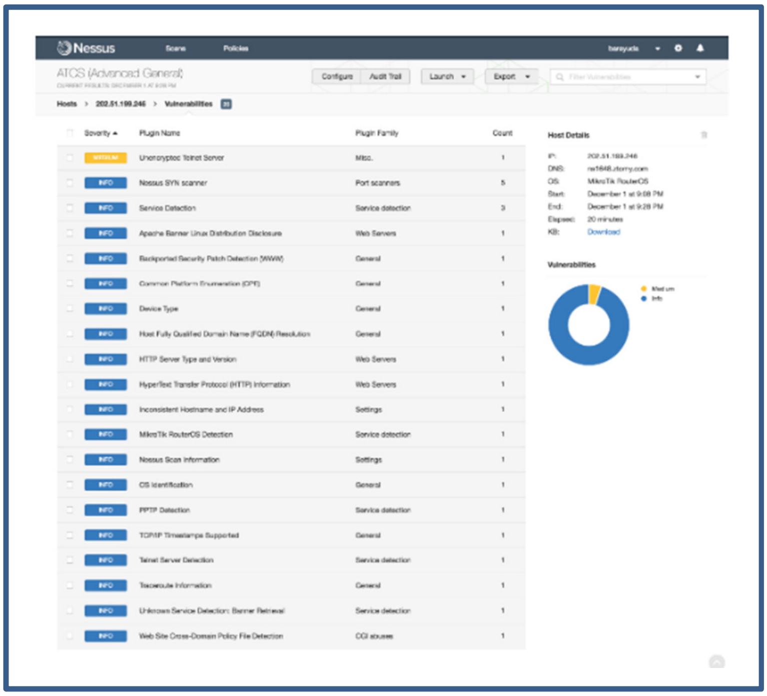


Figure 1. Schematic Nessus Analysis

4. RESULTS AND DISCUSSION

The initial step of this analysis is to start running Nessus vulnerability scanner with the aim of analyzing web ATCS Denpasar. The results of the analysis of the vulnerability of the web ATCS can be seen a few weak nesses that could be an entry point for attackers to take control of a web application. The results shown Nessus Scanner,:



ATCS (Advanced General)
CURRENT RESULTS: DECEMBER 1 AT 9:28 PM

Hosts > 202.51.199.246 > Vulnerabilities 20

Severity	Plugin Name	Plugin Family	Count
MEDIUM	Unencrypted Telnet Server	Misc.	1
INFO	Nessus SYN scanner	Port scanners	5
INFO	Service Detection	Service detection	3
INFO	Apache Banner Linux Distribution Disclosure	Web Servers	1
INFO	Backported Security Patch Detection (WWW)	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Server Type and Version	Web Servers	1
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1
INFO	Inconsistent Hostname and IP Address	Settings	1
INFO	MikroTik RouterOS Detection	Service detection	1
INFO	Nessus Scan Information	Settings	1
INFO	OS Identification	General	1
INFO	PPTP Detection	Service detection	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Telnet Server Detection	Service detection	1
INFO	Traceroute Information	General	1
INFO	Unknown Service Detection: Banner Retrieval	Service detection	1
INFO	Web Site Cross-Domain Policy File Detection	CGI abuses	1

Host Details

IP: 202.51.199.246
DNS: rw1648.ztorry.com
OS: MikroTik RouterOS
Start: December 1 at 9:08 PM
End: December 1 at 9:28 PM
Elapsed: 20 minutes
KB: Download

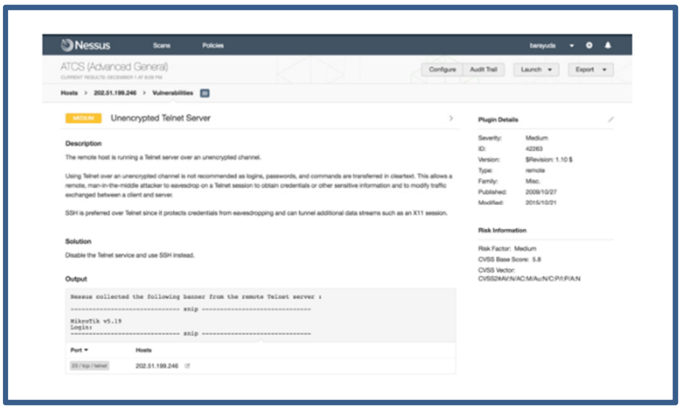
Vulnerabilities

Figure 2. Results scan of Nessus

From Figure 2 it can be seen kind of weakness, with details as follows:

1. 1 Total of category Medium
2. 19 Total of categories Info

A scan using the Nessus can also display detailed information of each category. Information displaying details of what caused the system weaknesses and suggestions to overcome these weaknesses. The information displayed is already grouped by cause of weakness. In figure 3 is shown a detail of a weakness in the Medium category.



ATCS (Advanced General)
CURRENT RESULTS: DECEMBER 1 AT 9:28 PM

Hosts > 202.51.199.246 > Vulnerabilities 20

MEDIUM Unencrypted Telnet Server

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Output

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------

MikroTik v5.19
Login:
------------------------------ snip ------------------------------
```

Port	Hosts
23 / tcp / telnet	202.51.199.246

Plugin Details

Severity: Medium
ID: 42263
Version: $Revision: 1.10 $
Type: remote
Family: Misc.
Published: 2009/10/27
Modified: 2015/10/21

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector:
CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Figure 3. Detail results Nessus Scanner

All the results of the scan using the Nessus is shown explanation about shortcomings. Contains an explanation of the weakness of the system can be used as a reference for the system administrator to fix that appears before uploaded on the web server. On the details are explained on the cause and also contains the solution. In the scan results above 1 d show the weakness of the scanner results that have been done are: Uncryptic Telnet Server. In addition to showing detailed weaknesses that could be the beginning of an attack for the attacker, scanner results also demonstrate solutions to overcome them. In the scan results indicated that a solution to overcome the weaknesses of the Disable the Telnet Service and use SSH instead. In the same way, can be known for weaknesses in other categories.

5. CONCLUTION

To take Conclusion of, the author uses the SWOT analysis with the following results:

STRENGHTS

1. Separating Server Application and Website Streaming Server
2. Using Mikrotik OS to run Live Streaming Video.
3. Using Ubuntu to run server Website

WEAKNESSES

1. Port Telnet to log into a proxy over IP is still open.
2. Viewed from a 404 error, it still uses a PHP framework (Code Igniter) is not Up-To-Date

OPPORTUNITIES

1. Using its own servers and use Mikrotik and Ubuntu OS
2. Port unneeded been closed

THREATS

1. Need to do updates to the PHP framework used and limited access to Telnet port used to connect to Mikrotik

ACKNOWLEDGMENT

Thank you for given the opportunity to examine more deeply the latest developments in information systems. The appreciation is awarded to all the colleagues who have given a lot of help both in discussion of ideas until the trial implementation stage of the study. Not forgotten also the appreciation is delivered to the ATCS Denpasar and Department of Electrical and Computer Engineering, Udayana University which has supported in lending the laboratory equipments in this research.

REFERENCES

[1]. Zaid Amin, Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer Di Pt. Sumeks Tivi Palembang (Paltv) Menggunakan Router Berbasis Unix.Vol 2 No.3. September 2012

[2]. http://atcs.denpasarkota.go.id , diakses 20 November 2016

[3]. Angir, Devi Christiani ,dkk.. Vulnerability Mapping pada Jaringan Komputer di Universitas X. Jurnal Infra Vol 3, No 2. 2015

[4]. https://www.tenable.com/products/nessusvulnerability-scanner, di akses 20 November 2016

BIBLIOGRAFI AUTHORS

Dr. Ir. Ni Wayan Sri Ariyani, MM.
Department of Electrical and Computer Engineering
Faculty of Engineering, Udayana University
Jimbaran Campuz, Bali - Indonesia

Ir. I Wayan Arta Wijaya, MErg.,MT.
Department of Electrical and Computer Engineering
Faculty of Engineering, Udayana University
Jimbaran Campuz, Bali - Indonesia