Research Article
Forbis: Journal Forensic Business Information Systems
Published online on: https://journal.universitasmulia.ac.id/index.php/forbis **1 (1) Januari 2024**

ANALISIS PERBANDINGAN METODE PTES DAN ISSAF SEBAGAI UJI KEAMANAN ROUTER DI ZURICH HOTEL BALIKPAPAN

Putra Prasetyo[1], Djumhadi[2], Wahyu Nur Alimyaningtias[3]*

[1,2,3] Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia

email: [1] putraprasetyo@students.universitasmulia.ac.id, [2] djumhadi@universitasmulia.ac.id, [3] wahyu.nur@universitasmulia.ac.id
[*]Correspondence

ARTICLE INFO

Article History
Received : 27 November 2023
Revised : 21 Januari 2024
Accepted : 22 Januari 2024
Available online : 22 Januari 2024

Keywords:
PTES
ISSAF
Router

Please cite this article in IEEE style as:

ABSTRACK

This research aims to determine the differences between the PTES and ISSAF methods as a router security test. This research is located at Zurich Hotel Balikpapan, where the router used for internet facilities is a core router that connects all devices, both internet users and servers belonging to Zurich Hotel. The conclusion in this study is that there are several differences, namely the PTES method focuses more on the target of attacks while ISSAF still requires other users as victims. The PTES method is also more flexible in its use while ISSAF has been determined for the assessment. Because the PTES method is more flexible the attack used also depends on the vulnerabilities found, while ISSAF has a more complete guide.

ABSTRAK

Penelitian ini bertujuan untuk mengetahui perbedaan metode PTES dan ISSAF sebagai uji keamanan router. Pada penelitian ini berlokasi di Zurich Hotel Balikpapan yang dimana router yang digunakan pada fasilitas internet merupakan core router yang menghubungkan semua perangkat baik pengguna internet dan server milik Zurich Hotel. Kesimpulan pada penelitian ini yaitu terdapat beberapa perbedaan yaitu metode PTES lebih fokus terhadap target serangan sedangkan ISSAF masih diperlukannya pengguna lain sebagai korban. Metode PTES juga lebih fleksibel dalam penggunaannya sedangkan ISSAF sudah ditentukan untuk assessmentnya. Dikarenakan metode PTES lebih fleksibel digunakan oleh karena itu serangan yang digunakan juga tergantung dengan kerentanan yang ditemukan sedangkan ISSAF terdapat panduan yang lebih lengkap.

1. Pendahuluan

Menurut informasi [1]setiap tahun pengguna internet semakin bertambah. Pada tahun 2020 terdapat 176 pengguna, 2021 terdapat 203 pengguna dan 2022 terdapat 205 juta yang menggunakan internet. Melihat kebutuhan internet yang semakin diperlukan, beberapa tempat umum juga menyediakan fasilitas untuk terhubung ke jaringan internet.

Salah satunya di Zurich Hotel Balikpapan yang menyediakan fasilitas untuk pengunjung agar dapat terhubung ke jaringan internet. Zurich Hotel Balikpapan bergerak dibidang industri pariwisata yang menyediakan pelayanan penginapan secara komersial. Tentunya banyak pengunjung yang menggunakan fasilitas ini untuk terhubung ke internet. Namun untuk mengelola fasilitas wifi tentu perlu diperhatikan juga keamanan jaringannya. Dikarenakan pengguna fasilitas ini bukan hanya dari pihak internal hotel Zurich saja maka akan bertambah juga peluang serangan yang terjadi pada jaringan.

Berdasarkan wawancara dengan IT Support, sejauh ini divisi yang bertugas menangani fasilitas internet di Zurich Hotel Balikpapan belum pernah melakukan uji keamanan pada fasilitas wifi dan belum memiliki work instructions terkait dengan keamanan jaringan yang dimana berfungsi sebagai petunjuk untuk melakukan uji keamanan perangkat jaringan, sehingga untuk keamanan jaringan hanya sebatas perkiraan saja. Kondisi seperti ini yang membuat keamanan pada jaringan kurang diperhatikan.

Pada jaringan komputer terdapat perangkat yaitu router yang berfungsi sebagai gateway untuk menyediakan layanan pengguna fasilitas wifi agar dapat terhubung ke jarinsgan internet. Dikarenakan fungsi dan perannya, router menjadi perangkat yang penting di jaringan komputer[2][3]. Hal ini menyebabkan router berpotensi menjadi target serangan. Oleh karena itu penelitian ini akan melakukan uji penetrasi pada router[4], [5].

Dikarenakan pihak hotel Zurich belum memiliki work instruction, maka dengan menggunakan metode uji penetrasi pihak hotel zurich memiliki acuan dan panduan untuk melakukan uji penetrasi pada router. Namun untuk mendapatkan hasil yang maksimal maka metode yang digunakan untuk uji penetrasi harus sesuai dengan kebutuhan pihak organisasi. Sehingga pemilihan metode juga penting dilakukan, karena setiap metode yang digunakan memiliki tahapan dan hasil yang berbeda. Beberapa penelitian yang telah dilakukan menyebutkan bahwa metode ini sangat berpengaruh terhadap langkah dan hasil dari pengujian sistem.

Pada penelitian ini menggunakan metode PTES (Penetration Testing Execution Standard) karena metode ini telah banyak digunakan untuk uji keamanan pada suatu sistem dan menggunakan metode ISSAF (Information Systems Security Assessment Framework) karena metode ini memiliki langkah-langkah yang spesifik terhadap target, yaitu router security assessment. Oleh karena itu kedua metode ini yang digunakan, sehingga peneliti tertarik untuk meneliti dengan judul "Analisis Perbandingan Metode PTES (Penetration Testing Execution Standard) dan Metode ISSAF (Information Systems Security Assessment Framework) Sebagai Uji Keamanan Router di Zurich Hotel Balikpapan".

2. Metode Penelitian

2.1. PTES

Terdapat 7 langkah dalam menggunakan metode PTES [6]–[8].

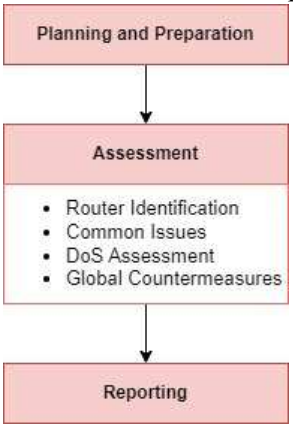
Gambar 1. Metode PTES

a. *Pre-Engagement*
Pada tahap ini juga menentukan kesepakatan tentang ruang lingkup, skenario pengujian, jenis pengujian dan waktu *penetration testing* kepada pihak internal hotel Zurich.

b. *Intelligence Gathering*
Melakukan pengumpulan informasi berupa status *port*, sistem operasi *router* yang digunakan, alamat *router* dan *hostname*.
c. *Threat Modelling*
Langkah ini melakukan penentuan jenis serangan yang akan digunakan berdasarkan informasi dari tahap sebelumnnya.
d. *Vulnerability Analysis*
Pada tahap ini melakukan pencarian untuk menemukan kelemahan lebih spesifik menggunakan *tools open source*.
e. *Exploitation*
Pada langkah ini dilakukan penyerangan atau eksploitasi pada target yang memanfaatkan kerentanan celah yang ada.
f. *Post Exploitation*
Tujuan tahap ini untuk mempertahakan akses yang telah diperoleh dan melakukan analisis terhadap infrastruktur sistem.
g. *Reporting*
Pada langkah ini membuat laporan terkait dengan hasil serangan dan memberikan solusi untuk bagaimana mengatasinya.

2.2. ISSAF

Menurut [9]–[12] terdapat tiga langkah untuk menggunakan metode *ISSAF* yaitu *planning and preparation*, *assessment* dan *reporting*.



Gambar 2. Metode ISSAF

a. *Planning and Preparation*
Pada tahap ini terdapat perjanjian atau kesepakatan sehingga ada perlindungan hukum bagi kedua belah pihak dan kesepakatan untuk waktu, tanggal dan ketentuan lainnya.
b. *Assessment*
Jika merujuk pada dokumen ISSAF 0.2.1 terdapat perbedaan tahapan *assessment* dengan objek lainnya. Berikut merupakan penilaian yang ada pada *router assessment*:
- *Router Identification*
Router identification merupakan proses untuk melakukan pencarian informasi seperti *hostname*, *scanning port* dan versi *OS*.
- *Common Issues Assessment*
Common issues yang digunakan pada penelitian ini adalah *HTTP, NTP, SNMP, TFTP, Password Security* dan *ARP Attack.*
- *Denial of Service Assessment*
Di tahap ini pengujian melakukan *denial of service* yang dimana *traffic* terhadap *router* dibanjiri sehingga menyebabkan *router* kehabisan *resource*.
- *Global Countermeasures*
Pada tahap ini melakukan pencarian solusi untuk mencegah kerentanan yang dapat menjadi ancaman.

c. ***Reporting***
Pada tahap ini melakukan laporan terkait apa saja yang telah dilakukan pada saat proses *penetration testing* dan kerentanan apa yang ditemukan.

2.3. Kebutuhan Sistem

Kebutuhan sistem merupakan penunjang terlaksananya penelitian ini, adapun kebutuhan tersebut ditampilkan pada tabel 1.

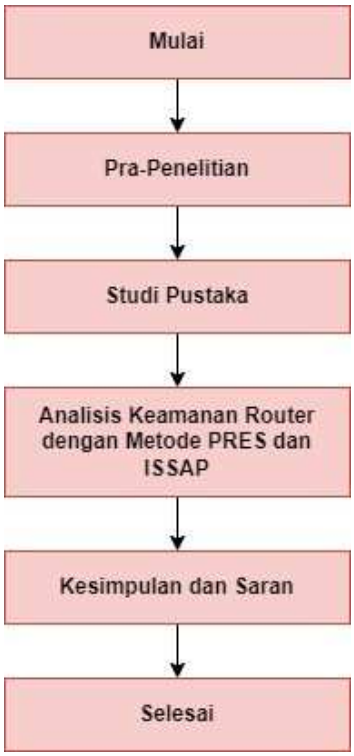
Tabel 1. Kebutuhan Sistem

Nama	Keterangan
Kali Linux	OS yang digunakan untuk pentest
Nmap	Software untuk port scanning
Hping3	Software untuk serangan DoS

Hydra	Software untuk serangan bruteforce
Snmpwalk	Software untuk serangan enumerasi pada protokol SNMP
Ntpdate	Software untuk sinkronisasi waktu dengan NTP target
Dsniff	Software untuk serangan ARP attack
Wireshark	Software untuk melihat paket saat serangan berlangsung

2.4. Alur Penelitian

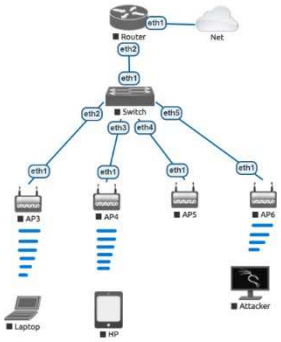
Alur penelitian merupakan suatu penuntun agar tahap-tahap untuk mencapai kesimpulan berjalan sesuai dengan *track* dan hasil yang tidak berubah-ubah, adapun alur penelitian sebagai berikut:



Gambar 3. Alur Penelitian

3. Hasil dan Pembahasan

Dalam proses pengujian serangan untuk menguji metode PTES dan ISSAF, disini menggunakan rancangan topologi sebagai berikut untuk menggambarkan posisi penyerang. Adapun topologi ditampilkan pada gambar 4.



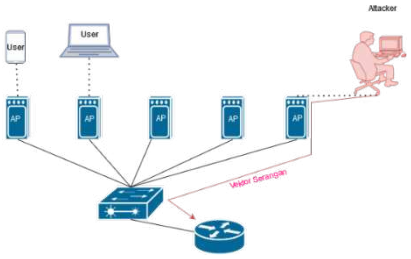
Gambar 4. Desain Topologi

Gambar diatas merupakan posisi attacker yang akan melakukan penetrasi terhadap router. Attacker diposisikan sama dengan pengguna fasilitas wifi lainnya.

3.1 PTES

a. Pre-Engagement

Pengujian dilakukan dalam sehari pada pukul 09:00 sampai dengan pukul 17:00. Semua jines serangan diperbolehkan termasuk *stress testing*.



Gambar 5. Vektor Serangan

Gambar diatas merupakan arah serangan ke perangkat *router* dari titik serangan yang dimana posisi *attacker* terhubung melalui jaringan *wireless* seperti pengguna lainnya. Dapat dilihat titik serangan dimulai dari *attacker* yang diposisikan sama dengan pengguna lainnya.

b. *Inteliegence Ghathering*

Didapatkan informasi target menggunakan sistem operasi *RouterOS* dengan versi 6.49.6. jaringan di area *lobby* adalah 255.255.255.0 atau /24 yang berarti *IP gateway* adalah 192.168.20.1/24 yang merupakan *IP* dari target. Sedangkan di area *room* informasi yang

didapatkan terkait dengan jaringan yang digunakan adalah 130.0.0.0/15.

Tabel 2. Detail Port

Port	State	Service
21	Open	FTP
22	Open	SSH
23	Open	Telnet
53	Open	Domain
80	Open	HTTP
2000	Open	Cisco
8291	Open	Unkown
53	Open	Domain
67	Open | Filtered	DHCPS
68	Open | Filtered	DHCPC
123	Open | Filtered	NTP

Pada tabel diatas merupakan hasil *scanning* protokol *TCP* dan *UDP* dari kedua jaringan.

c. *Threat Modelling*

Dari hasil tahapan sebelumnya yaitu *inteliegence gathering* yaitu mendapatkan informasi berupa status *port* dari target serangan perangkat *router.* Serangan yang digunakan adalah *bruteforce* terhadap *service ssh* dan *telnet* sampai dengan *DoS Attack.*

d. *Vulnerability Analysis*

Pada tahap ini melakukan analisis kerentanan pada target menggunakan *Nmap*. Hasil *vulnerability scanning* dari titik serangan di kedua jaringan yaitu 192.168.20.0/24 dan 130.0.0.0/15 target memliki kerentanan pada protokol *HTTP port* 80 dengan jenis serangan *Denial of Service Attack* dengan *CVE-2011-1002.*

e. Exploitation

Hasil akhir jenis serangan yang digunakan pada saat penetration testing dari kedua titik serangan yaitu jaringan 192.168.20.0/24 dan 130.0.0.0/15. Adapun detail hasil exploitation ditunjukkan pada tabel 3.

Tabel 3. Exploitation PTES

Jenis Serangan	Status
Port Scanning	Berhasil
Brute Force	Gagal
DoS	Berhasil

f. *Reporting*

Terdapat kerentanan yang dimana dari titik serangan *service* untuk autentikasi dapat diakses oleh seluruh pengguna internet di Zurich Hotel, hal ini dapat menyebabkan *router* dapat diambil alih oleh pengguna yang tidak bertanggung jawab. Untuk pengujian *DoS* dapat membuat target *down* sehingga *router* tidak dapat beroperasi.

3.2 ISSAF

a. Planning and Preparation

Kedua belah pihak menyetujui aturan-aturan *penetration testing*. Berikut merupakan aturan *penetration testing*:

- Waktu di Zurich hotel Balikpapan pukul 08:00 sampai dengan 17:00 di Zurich Hotel Balikpapan.
- Target serangan merupakan *core router* yang berfungsi sebagai pusat penghubung semua jaringan di Zurich Hotel Balikpapan.
- Pengujian *stress testing* atau jenis serangan *DoS* diperbolehkan.
- Peneliti diperbolehkan untuk mengunggah dan mengunduh *file* pada target.
- Peneliti dilarang merubah konfigurasi pada target baik itu dengan autentikasi atau tanpa autentikasi.
- Peneliti tidak bertanggung jawab jika terdapat serangan yang bukan disebabkan oleh peneliti pada saat *penetration testing.*

b. *Assessment*

- *Router Identification*
  Didapat informasi jaringan yang digunakan pada *lobby area* adalah

192.168.20.0/24 dengan IP target 192.168.20.1/24. Perangkat *router* yang digunakan adalah mikrotik dengan *RouterOS* versi 6.49.6. *Hostname* dari target adalah ITzurich. Sedangkan pada *room area* didapatkan informasi jaringan yang digunakan adalah 130.0.0.0/15 dan *IP* target adalah 130.0.0.1/15.

Tabel 4 Router Identification

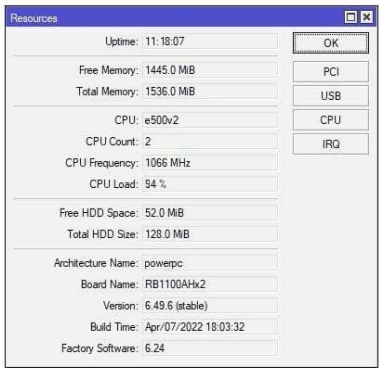
Port	**Status**
HTTP	Open
NTP	Open | Filtered
SNMP	-
TFTP	-
Telnet	Open
SSH	Open

- *Common Issues Assessment*
  Tabel 4.3 Common Issues Assessment

Tabel 5. Common Issues Assessment

Assessment	**Hasil**
HTTP	Gagal
NTP	Gagal
Password Security	Telnet (Berhasil) SSH (Gagal)
ARP Attack	Berhasil

- *DoS Assessment*
  Jenis serangan *denial of service attack* dapat membuat *down* target, sehingga *IT Support* Zurich Hotel tidak dapat mengakses perangkat *router*. Hal ini juga dapat mempengaruhi performa perangkat lainnya yang terhubung dengan target *router* dikarenakan *router* tidak dapat melayani akibat *overload* yang disebabkan lalu lintas jaringan yang tinggi mengarah ke *router*.



Gambar 6. CPU Load

- *Global Counter Measures*

Tabel 6. Global Counter Measures

Vulnerablity	**Mitigation**
Telnet	Telnet tidak didukung dengan enkripsi, sehingga paket yang lewat dapat dilihat secara plain text. Terdapat service lain untuk akses ke perangkat router yang lebih baik yaitu menggunakan service SSH atau yang mendukung enrkripsi.
ARP Attack	Perangkat router target menggunakan MikroTik yang dimana terdapat fitur ARP Watch yang dapat digunakan secara gratis.

c. Reporting

Pada pengujian menggunakan metode *ISSAF (Information Systems Security Assessmen Framework) router security assessment*, terdapat beberapa *assessment* yang berhasil dan gagal.

Tabel 7. Reporting

Assessment	**Hasil Serangan**
HTTP	Gagal
NTP	Gagal

Password Security	Telnet (Berhasil) SSH (Gagal)
ARP Attack	Berhasil
DoS	Berhasil

4. Kesimpulan

Kedua metode sama-sama efektif karena sesuai dengan apa yang direncanakan. Namun untuk efesiensi, metode PTES (Penetration Testing Execution Standard) lebih efisien. Hal ini dikarenakan metode PTES (Penetration Testing Execution Standard) lebih fleksibel, sehingga jenis serangan yang digunakan dapat lebih banyak sesuai dengan jenis kerentanan yang ditemukan. Namun untuk menggunakan metode PTES (Penetration Testing Execution

5. Referensi

[1] P. Studi Ilmu Komunikasi, "Tren Penggunaan Media Sosial Selama Pandemi Di Indonesia," 2020.

[2] A. I. Haris, B. Riyanto, F. Surachman, And A. A. Ramadhan, "Analisis Pengamanan Jaringan Menggunakan Router Mikrotik Dari Serangan Dos Dan Pengaruhnya Terhadap Performansi," *Komputika : Jurnal Sistem Komputer*, Vol. 11, No. 1, Pp. 67–76, Jan. 2022, Doi: 10.34010/Komputika.V11i1.5227.

[3] I. Budi, J. Teknik Informatika, S. Balikpapan, J. Letjen Zaini Azhar Maulani No, And K. Balikpapan, "Perancangan Alat Monitor Penggunaan Laboratorium Komputer Dan Laboratorium Network Berbasis Rfid Di Stmik Balikpapan," Vol. 2, No. 2, 2018.

[4] A. Wijayanto, I. Riadi, Y. Prayudi, And T. Sudinugraha, "Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, Vol. 8, No. 2, Pp. 156–169, Jul. 2022, Doi: 10.26594/Register.V8i2.2953.

[5] A. Wijayanto, I. Riadi, And Y. Prayudi, "Taara Method For Processing On The Network Forensics In The Event Of An Arp Spoofing Attack," *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*, Vol. 7, No. 2, Pp. 208–217, Mar. 2023, Doi: 10.29207/Resti.V7i2.4589.

[6] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, And M. T. Farizky, "Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard)," *Jurnal Komputer Dan Informatika*, Vol. 11, No. 1, Pp. 91–95, Mar. 2023, Doi: 10.35508/Jicon.V11i1.9809.

[7] F. Y. Fauzan And S. Syukhri, "Analisis Metode Web Security Ptes (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, Vol. 9, No. 2, P. 105, Jun. 2021, Doi: 10.24036/Voteteknika.V9i2.111778.

[8] S. Utoro *Et Al.*, "Analisis Keamanan Website E-Learning Smkn 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard."

[9] E. S. Prasetyo And N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf," *Jurnal Ilmiah Informatika*, Vol. 9, No. 2, Pp. 82–86, Sep. 2021, Accessed: Feb. 07, 2023. [Online]. Available: Https://Ejournal.Upbatam.Ac.Id/Index.Php/Jif/Article/View/3758

[10] A. W. Wardhana And H. B. Seta, "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode Issaf Pada Website Universitas Xyz," *Informatik : Jurnal Ilmu Komputer*, Vol. 17, No. 3, P. 226, Dec. 2021, Doi: 10.52958/Iftk.V17i3.3653.

[11] G. Guntoro, L. Costaner, And M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *Jipi (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, Vol. 5, No. 1, P. 45, Jun. 2020, Doi: 10.29100/Jipi.V5i1.1565.

[12] S. Eko Prasetyo And N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf," *Jurnal Ilmiah Informatika*, Vol. 9, No. 02, Pp. 82–86, Sep. 2021, Doi: 10.33884/Jif.V9i02.3758.