BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Penelitian ini memiliki tujuan untuk melakukan pengujian jaringan *wireless* menggunakan metode *PTES* di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal. Pada penelitian yang telah dilakukan sebelumnya akan membantu untuk penelitian selanjutnya agar dapat menghasilkan penelitian yang lebih baik lagi.

Pada penelitian [10] oleh Haeruddin dan Arif Kurniadi (2020) melakukan penelitian menggunakan metode *Penetration Testing* untuk analisis keamanan jaringan *WPA2-PSK* pada TP-Link Archer A6. Penelitin ini menggunakan jenis serangan *Cracking The Encryption, Bypassing MAC Address Authentication, DoS Attack* dengan kali linux. Berdasarkan hasil pengujian ditemukan masih banyak kelemahan pada sistem, karena masih menggunakan konfigurasi *default* dari *vendor* dan dari ketiga jenis serangan tersebut hanya satu menunjukan hasil status gagal yaitu serangan *Bypassing MAC Address Authentication*. Hasil ini menunjukkan bahwa konfigurasi secara *default* masih rentan keamanannya.

Pada penelitian [1] oleh Bita P.Z., dkk. (2020) melakukan penelitian menggunakan metode *penetration testing* untuk analisis *security assessment* dengan fokus pada keamanan *webserver* untuk menjaga kapabilitas keamanan teknologi informasi pertahanan negara untuk menjaga dari serangan siber seperti *ransomeware, trojan policy, dan policy*. Penelitian dilakukan di Pusat Pertahanan Siber Kemeneterian Pertahanan dan Lab Siber Unhan. Tahapan *penetration* dilakukan setelah melakukan analisis *vulnerability* dengan melakukan *SQL Injection* diperoleh hasil setelah dilakukan *scanning* terdapat *port* 22 sebagai *SSH*, *port* 80 *HTTP*, dan *port* 3306 *MYSQL*, terdapat celah kerentanann dan tahap uji kerentanan menggunana standar *Open Web Application Security Project* (*OWASP*)

serta metode *Common Vulnerability Scoring System* (*CVSS*). Setelah melakukan uji *penetration testing* pada IP 139.2*5.2*5.2 sistem *firewall* pada *webserver* ini cukup baik sehingga cukup menyulitkan dalam mengeksploitasi sistem, namun pada sistem operasi pada *webserver* menggunakan *Apache/2.4.18 Ubuntu* dapat diketahui dengan ditemukan 3 akses *login* yang bisa menjadikan penyerang masuk ke sistem *webserver* dengan masuk melalui celah *user ID* dan akses *database*.

Pada penelitian [12] oleh M. I. Rusdi dan D. Prasti (2019) melakukan penelitian menggunakan metode *Penetration Testing* untuk analisis Jaringan *Wifi*. Penelitian ini menggunakan sistem operasi kali linux dengan menganalisa sistem keamanan *WPA-PSK, WPA2-PSK* dan masih ditemukan celah keamannya karena konfigurasi *wireless LAN* menggunakan *default* dari *vendor*. Hal ini dibuktikan dari hasil perocbaan serangan metode *brute force attack password* dari *wifi* masih dapat di *crack* yang dapat memudahkan para penyusup untuk memanfaatkan jaringan tersebut secara ilegal.

Pada penelitian [13] oleh A. Kholiq dan D. Khoirunnisa (2019) melakukan penelitian menggunakan metode *Penetration Testing* untuk analisis keamanan jaringan *wireless* di PT. Win Prima Logistik. Dalam penelitian ini menggunakan sistem operasi kali linux dengan melakukan empat jenis serangan yaitu serangan *WPS* aktif, *Bypassing MAC Address, ARP Spoofing, Cracking The Encryption*. Berdasarkan hasil pengujian masih ditemukan celah keamannya yang mudah dieksploitasi untuk mendapatkan akses secara ilegal, dibuktikan dengan hasil yang didapat dua dari empat jenis serangan mendapatkan status berhasil serta dua serangan gagal yang dapat di uji coba menggunakan jenis serangan dengan *tools* lainnya.

Pada penelitian [14] oleh Aditia (2019) dalam penelitian tugas akhirnya melakukan analisis keamanan jaringan *wireless* di IT Telkom Purwokerto menggunakan metode *Penetration Testing*. Pada penelitian ini masih ditemukan celah keamanan jaringan yang dapat dieksploitasi melalui jenis serangan *attacking the infrastructure* (*DoS Attack*). Pada penelitian ini terdapat jenis serangan yang tidak berhasil yang dapat dikembangkan lagi untuk mengevaluasi jaringan *wireless* dengan menggunakan *tools* atau teknik penyerangan lainnya agar mendapatkan hasil analisis yang lebih maksimal.

Pada penelitian [9] oleh Desi Maya Sari, dkk (2017) melakukan penelitian menggunakan metode *Penetration Testing* untuk analisis sistem keamanan jaringan *wireless* (*WEP,WPAPSK/WPA2PSK*) *Mac Address* di Laboratorium Sistem Multimedia dan AI Jurusan Teknik Informatika Fakultas Teknik UHO. Pada penelitian ini menggunakan sistem operasi kali linux bahwa keamanan yang dimiliki mempunyai kelemahan dengan masih banyak celah yang bisa diekspolitasi. Hal ini dapat dibuktikan dari hasil penelitian yang diperoleh dari tiga jenis serangan yaitu *Cracking The Encryption (WEP), Cracking The Encryption (WPA), Bypassing WLAN Authentication* masing-masing sebanyak tiga kali percobaan diperoleh hanya dua yang mendapatkan status gagal yaitu pada serangan *Cracking The Encryption (WPA*) yang artinya masih terdapat celah keamanan yang belum bisa memberikan keamanan jaringan ketika melakukan akses internet pada jaringan yang sama.

Berikut ini merupakan rangkuman mengenai penelitian sebelumnya yang akan dijadikan sebagai acuan dalam penelitian yang penulis lakukan, dapat dilihat pada tabel 2.1:

Tabel 2. 1 Penelitian Sebelumnya

No	Judul	Masalah	Jenis Serangan	Penulis	Perbedaan	Hasil
1	Analisis Keamanan Jaringan *WPA2-PSK* Menggunakan Metode *Penetration Testing* (Studi Kasus : TP-Link Archer A6)	Konfigurasi *default* dari vendor masih banyak digunakan	*Cracking the encryption, Bypassing mac authentication, Dos attack*	Haeruddin, Arif Kurniadi (2021)	Tidak mengamankan celah kerentanan yang ditemukan	Konfigurasi bawaan vendor atau *default* memiliki kerentanan/mudah diretas.
2	Analisis *Security Asessment* Menggunakan Metode *Penetration Testing* Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara	Maraknya kasus pencurian data pada *webserver* dan *database*	*SQL Injection*	Bita Parga Zen, Rudy A.G.G, Agus H.S.R (2020)	Menggunakan standar acuan *OWASP* dan *CVSS*	uji penetration testing pada IP 139.2*5.2*5.2 sistem *firewall* pada *webserver* ini cukup baik , namun pada sistem operasi pada *webserver* menggunakan *Apache/2.4.18 Ubuntu* dapat diketahui dengan ditemukan 3 akses *login*
3	*Penetration Testing* Pada Jaringan *Wifi* Menggunakan Kali Linux	Eksplorasi fitur keamanan *WPA-PSK* dan *WPA2-PSK* jaringan *wifi* menggunakan sistem operasi kali linux	*Brute force password attack*	M. I. Rusdi, D. Prasti	Menggunakan tahap penelitian Tindakan atau *action research*, tidak mengamankan celah yang ditemukan	Jaringan *wireless* dengan konfigurasi *default* dapat mudah masuknya penyusup

No	Judul	Masalah	Jenis Serangan	Penulis	Perbedaan	Hasil
4	Analisis Keamanan *Wireless Local Area Network* (*WLAN*) Dengan Metode *Penetration Testing Execution Standard* (*PTES*) Studi Kasus : PT. Win Prima Logistik	Fitur keamanan yang rendah dengan banyaknya data penting perusahaan	*WPS* aktif, *Bypassing mac authentication, arp spoofing, cracking the encryption*	A. Kholiq dan D. Khoirunnisa (2019)	Studi kasus serta *tools* yang dipakai	Celah keamanan ditemukan dengan teknik serangan *bypassing MAC address* dan *ARP Spoofing*.
5	Analisis Keamanan Jaringan *Wireless* Menggunakan Metode *Penetration Testing*. (Studi Kasus : IT Telkom Purwokerto)	Menemukan celah kerentaanan yang tersedia	*Attacking the infrastructure*	Aditia (2019)	*Tools* yang digunakan untuk mencari celah keamanan serta hanya simulasi menggunakan dua komputer saja.	Celah keamanan yang ditemukan hanya sedikit
6	Analisis Sistem Keamanan Jaringan *Wireless* (*WEP, WPAPSK/WPA2PSK*) *Mac Address* Menggunakan Metode *Penetration Testing*	Jaringan *wireless* masih bisa diserang walaupun memiliki sistem keamanan jaringan	*Cracking the encryption, Bypassing mac authentication*	Desi Maya Sari, dkk (2017)	Perangkat lunak yang digunakan	Serangan keamanan *WPA* menemui kegagalan 2 kali dari 3 percobaan.

Berdasarkan enam penelitian tersebut, maka penulis menyimpulkan bahwa untuk pengujian sistem keamanan jaringan diperlukan sebuah teknik serta jenis serangan yang berbeda-beda dan menggunakan pedoman uji

penetrasi untuk mendapatkan hasil penelitian yang baik. Perbedaan antara penelitian ini dengan yang lain adalah melakukan pengujian keamanan jaringan *wireless* pada sebuah kantor balai desa yang berada di Kalisapu Kecamatan Slawi Kabupaten tegal menggunakan *framework penetration testing* atau standar acuan PTES serta melakukan uji penetrasi dengan sistem operasi kali linux pada *virtual machine* dengan bantuan *tools* seperti *aircrack-ng* dan *mdk3* dengan pengujian sebanyak 5 kali pada setiap uji penetrasi jaringan.

2.2 Dasar Teori

2.2.1 Sistem Jaringan Komputer

Jaringan komputer adalah jaringan telekomunikasi antara dua *device* atau lebih yang saling terhubung sehingga dapat bertukar data atau informasi[15]. Jaringan komputer dapat dikatakan terkoneksi apabila *device* yang ada dalam jaringan memiliki perangkat kartu jaringan yang dapat dihubungkan secara *wired* (kabel) atau *wireless* (nirkabel) sehingga bisa saling bertukar data/informasi dan berbagi sumber daya yang dimiliki[15]. Jaringan komputer terbagi menjadi beberapa jenis berdasarkan cakupan areanya[16], yaitu :

1. *Local Area Network* (LAN)

   Local Area Network atau *LAN* merupakan sebuah konsep jaringan komputer untuk menghubungkan komputer melalui perangkat jaringan dalam cakupan area yang kecil yang dapat di aplikasikan untuk kantor, sekolah atau rumah yang cenderung memakai koneksi kabel *ethernet* maupun teknologi jaringan nirkabel (*wireless*) yang dikenal dengan nama jaringan *wifi* atau *Wireless LAN* (*WLAN*).

2. *Metropolitan Area Network* (MAN)

   Metropolitan Area Network atau *MAN* merupakan sebuah konsep jaringan komputer untuk menghubungkan komputer melalui perangkat jaringan dalam cakupan area yang besar antar perkotaan.

3. *Wide Area Network* (WAN)

Wide Area Network atau *WAN* merupakan sebuah konsep jaringan komputer untuk menghubungkan komputer melalui perangkat jaringan dalam cakupan area yang lebih luas seperti antar negara maupun benua.

2.2.2 Jaringan Wireless LAN

Wireless Local Area Network (*WLAN*) adalah jaringan komputer yang menggunakan frekuensi radio dan *infrared* sebagai media transmisi data. *WLAN* sering disebut sebagai jaringan nirkabel atau jaringan *wireless*. Proses komunikasi tanpa kabel ini dimulai dengan munculnya peralatan berbasis gelombang radio, seperti *walkie-talkie, remote control*, ponsel dan perangkat radio lainnya. Kebutuhan untuk menjadikan komputer sebagai barang yang mudah dibawa (*mobile*) dan mudah digabungkan dengan jaringan yang sudah ada yang akhirnya mendorong pengembangan teknologi *wireless* untuk jaringan komputer.

WLAN sebenarnya hampir sama dengan jaringan *LAN*, akan tetapi setiap perangkat atau *node* yang terhubung pada *WLAN* menggunakan *wireless device* untuk saling bertukar data/informasi serta memiliki dua *mode* konfigurasi yang dapat digunakan yaitu infrastruktur dan *Ad-Hoc*. Konfigurasi infrastrukur merupakan komunikasi antar masing-masing *Personal Computer* (*PC*) melalui sebuah *access point* pada jaringan *WLAN*. Perangkat yang terhubung dengan *WLAN* menggunakan *channel* frekuensi dan *SSID* yang sama[16].

2.2.3 Sistem Keamanan Jaringan Komputer

Keamanan jaringan adalah konfigurasi yang berfungsi untuk melindungi data, menjaga kerahasiaan, integritas, serta menjamin ketersediaan akses jaringan komputer, dalam keamanan jaringan terdapat

beberapa aspek apabila sebuah jaringan komputer disebut aman jika memenuhi kategori berikut ini[13]:

1. *Confidentiality* (Kerahasiaan)

   Aspek untuk melindungi suatu informasi dengan membatasi pihak ketiga yang akan mengakses ke informasi tersebut hanya pengirim dan penerima yang mengetahuinya.

2. *Integrity* (Integritas)

   Aspek menjamin informasi atau data bisa konsisten, akurat dan terjaga tidak dapat diubah oleh pihak lain dan hanya bisa diubah oleh pengirim atau penerima.

3. *Authentication*

   Mengutamakan validitas dari pengguna informasi atau data yang valid berasal dari *server* asli yang diakses.

4. *Availability*

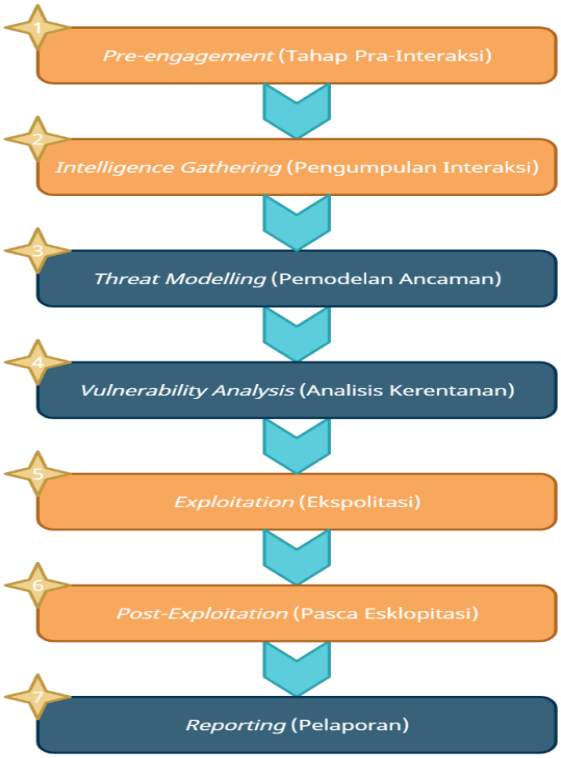
   Layanan informasi atau data dapat diakses kapanpun dan terjamin ketersediannya ketika akan digunakan.

5. *Non Repudiation*

   Aspek yang berkaitan dengan pencataan pengguna, ketika melakukan akses ke sistem atau jaringan pengguna tidak dapat menyangkal telah masuk ke sistem atau jaringan tersebut.

2.2.4 Penetration Testing

Penetration testing merupakan bagian dari jenis *ethical hacking* yaitu sebuah metode serta prosedur untuk menguji keamanan informasi. *Penetration testing* adalah aktivitas untuk mengevaluasi sebuah sistem yang sudah ada dengan melakukan serangan untuk mengetahui celah keamanan pada sistem tersebut[17]. Dalam keamanan jaringan *wireless*, *penetration testing* digunakan untuk menambahkan *firewall* pada *router* yang dapat mengurangi resiko kerentanan sistem atau data yang terdapat didalamnya. *Penetration testing* memiliki standar atau pedoman yang dapat digunakan sebagai acuannya atau biasa disebut *Penetration Testing Execution Standard* (*PTES*) yang dibuat tahun 2010 oleh para praktisi *computer security*.



Gambar 2. 1 Tahapan *Penetration Testing Execution Standard*

Pada gambar 2.1 merupakan gambaran tahap dari uji penetrasi *PTES*, standar ini memungkinkan seorang *pentester* dapat fokus mengeksploitasi area yang rentan dan memilih teknik serangan yang sesuai[18]. *PTES*

dirancang untuk mengatasi kekurangan dalam pengujian penetrasi jarinngan dengan memberikan panduan tentang alat, teknik, dan elemen yang akan dilakukan pengujian[19]. Melalui pengumpulan informasi dan model ancaman dimana penguji dapat melakukan pengujian secara detail untuk mendapatkan informasi yang lebih banyak melalui penelitian kerentanan, eksploitasi dan pasca eksploitasi dimana semua tahap itu dilakukan dan akhirnya dilanjutkan dengan membuat laporan yang menangkap seluruh proses. *PTES* memiliki beberapa tahapan sebagai berikut[20]:

1. *Pre-Engagement* (Pra Interaksi)

   Tahap persiapan atau kesepakatan yang dilakukan *pentester* kepada pemilik layanan agar tidak terjadi permasalahan pelanggaran hukum dan kebijakan.

2. *Intelligence Gathering* (Pengumpulan Informasi)

   Tahap pengumpulan informasi yang dapat membantu proses *penetration testing* yang dapat diambil dari beberapa metode yang pada penelitian ini berfokus *penetration test* keamanan jaringan *wireless*.

3. *Threat Modelling* (Pemodelan Ancaman)

   Tahap untuk melakasanakn *penetration test* yang benar dengan melakukan pendekatan pemodelan ancaman agar lebih mudah menentukan serangan ke pemilik layanan yang dalam penelitian ini adalah serangan ke sistem jaringan *wireless*.

4. *Vulnerability Analysis* (Analisis Kerentanan)

   Tahap mencari dan menganalisa informasi kerentanan sistem jaringan *wireless* guna mempermudah dalam proses uji penetrasi yang diperoleh berdasarkan informasi yang didapatkan dari metode yang digunakan sebelumnya.

5. *Exploitation* (Eksploitasi)

   Tahap melakukan *penetrasi test* masuk ke sistem jaringan *wireless* untuk mengetahui celah keamanan jaringan dengan metode yang digunakan namun dilakukan setelah mengetahui celah keamanan

yang bisa digunakan serta serangan yang dilakukan akan berhasil atau gagal.

6. *Post Exploitation* (Pasca Ekspoitasi)

   Tahap menyusun rencana setelah proses eksploitasi serta melakukan analisis bagian yang paling rentan dan menjelaksan bagian yang terkena resiko serta dampaknya dan memastikan prosedur yang disepakati sebelumnya dapat digunakan selama tahap pasca eksploitasi.

7. *Reporting* (Pelaporan)

   Tahap menyajikan laporan hasil setelah dilakukan uji penetrasi dengan melaporkan resiko yang ditemukan dan bagaimana rekomendasi penanggulangan resiko pada celah yang ditemukan.

2.2.5 Oracle VM Virtualbox

Oracle *Virtual Machine Virtualbox* adalah perangkat lunak virtualisasi yang dapat digunakan untuk mengeksekusi sebuah sistem operasi tambahan di dalam sistem operasi utama. *Virtual machine* dikembangkan untuk meminimalisir penggunan komputer serta dengan penggunaan ini seseorang dapat bekerja layaknya menggunakan komputer nyata[21]. Dengan adanya *virtual machine* ini pengguna tidak perlu untuk melakukan instal ulang komputer cukup dengan menjalankan sistem operasi yang sudah terinstal di dalam sebuah *VM virtual box*.

2.2.6 Kali linux

Kali linux adalah sebuah distro sistem operasi yang berbasis debian linux yang banyak digunakan untuk penetrasi jaringan. Kali linux merupakan salah satu distro linux yang dirancang untuk keperluan penetrasi jaringan serta sebuah sistem keamanan pada komputer, kali linux bersifat *open source* yang artinya bisa digunakan bebas oleh siapa saja tanpa perlu membeli lisensi. Dalam sistem operasi ini terdapat sekitar 300 alat lebih yang dapat digunakan untuk keperluan *penetration testing*[22].

2.2.7 *Brute Force*

Brute force adalah suatu metode untuk meretas suatu *password* dengan mencoba semua kemungkinan kombinasi kata pada *wordlist*. *Wordlist* merupakan sekumpulan *password* yang kemungkinan digunakan pada sebuah sistem keamanan jaringan. Metode *brute force* membutuhkan waktu cukup lama tergantung kombinasi kata yang tersedia pada sebuah *wordlist*[23].

2.2.8 *Cracking The Encryption*

Cracking the encryption adalah jenis serangan untuk mengeksploitasi dan menguji tingkat kekuatan *password* yang digunakan pada sistem keamanan jaringan *wireless*, jenis serangan ini dapat mengetahui *password* yang sedang digunakan oleh jaringan tersebut[10]. Pada jenis serangan ini membutuhkan sebuah *wordlist* dan paket *handshake*, paket *handshake* merupakan sebuah paket yang diperoleh saat proses pengguna masuk kedalam sebuah jaringan.

2.2.9 *Router Attack*

Router attack merupakan jenis serangan untuk menyerang sebuah infrastukur jaringan yang dirancang untuk melemahkan atau mengganggu aktivitas sebuah infrastruktur jaringan[10].