BAB III. LANDASAN TEORI

Pada landasan teori akan dipaparkan beberapa istilah yang digunakan dalam pengujian ini.

3.1. Sistem

Sistem Sistem adalah kumpulan dari suatu komponen yang memiliki unsur dan saling berhubungan anta satu dengan yang lainnya untuk mencapai suatu tujuan. Menurut Sutanto dalam Djahir dan Pratita (2015) sistem merupakan suatu kumpulan dari subsistem apapun dan dapat berupa fisik maupun non-fisik yang saling berhubungan dan bekerjasama antara satu dengan yang lainnya demi mencapai satu tujuan tertentu [11]. Sedangkan menurut Mulyani (2016) sistem adalah kumpulan sub-sistem yang saling bekerja sama dengan tujuan yaitu mengeluarkan *output* yang sudah ditentukan [12]. Menurut Hutahean (2015) menyatakan bahwa sistem adalah suatu jaringan kerja dari prosedur yang saling berhubungan satu sama lain, berkumpul bersama-sama untuk melaksanakan sasaran yang sudah ditentukan [13].

3.2. Informasi

Informasi merupakan sebuah data yang telah diolah sehingga memiliki suatu arti yang bermakna bagi seseorang ataupun organisasi. Menurut Sutanta (2011) Informasi adalah hasil dari pengolahan data sehingga memiliki makna bagi penerima informasi sehingga penerima dapat mengambil keputusan selanjutnya berdasarkan data yang didapat [14]. Sedangkan menurut William (2007) Informasi adalah suatu data yang sudah dimanipulasi sehingga menjadi bentuk lain yang dapat digunakan untuk mengambil keputusan [15]. Menurut Fajri (2014) Informasi dapat berupa data yang telah diproses dan diubah sehingga menjadi lebih berarti dan dapat

digunakan sebagai pengambil keputusan yang yakin [16].

3.3. Sistem Informasi

Sistem Informasi merupakan sebuah sistem pada suatu organisasi dimana data diolah menjadi suatu informasi yang berguna untuk mengambil keputusan selanjutnya. Menurut Kertahadi (2007) Sistem Informasi adalah sebuah alat untuk menyajikan informasi sedemikin rupa sehingga bermanfaat bagi penerimanya, dan memiliki tujuan untuk memberikan informasi dalam perencanaan, memulai, pengorganisasian, operasional sebuah perusahaan yang melayani sinergi organisasi dalam proses mengendalikan pengambilan keputusan [17]. Sedangkan menurut Tata Sutabri, S.Kom., MM (2005) menyatakan bahwa sistem informasi merupakan sebuah sistem didalam suatu organisasi yang mempertemukan pengolahan transaksi harian yang mendukung fungsi organisasi manajerial agar dapat menyediakan laporan kepada pihak yang memerlukan [18]. Sedangkan menurut O'Brien (2005) Sistem Informasi adalah suatu kombinasi antar orang, perangkat keras, perangkat lunak, jaringan komputer, jaringan komunikasi dan database yang menyebarkan, mengubah dan mengumpulkan informasi dalam organisasi [19].

3.4. Peretasan (*Hacking*)

Peretasan merupakan sebuah tindakan untuk memasuki sebuah sistem operasional. Peretasan dapat bersifat baik maupun buruk, peretas baik memasuki sebuah sistem guna mencari celah agar tidak dapat dimasuki oleh peretas buruk sedangkan peretas buruk dapat mengeksploitasi data-data yang dimiliki sebuah sistem operasional secara ilegal. Orang yang melakukan peretasan biasa disebut peretas (*Hacker*). Menurut Dr. Bambang Sugiantoro (2019) *hacking* adalah sebuah teknik yang dilakukan seseorang guna menyerang suatu sistem dengan mengeksploitasi kelemahan-kelemahan yang dimiliki oleh sistem tersebut untuk mendapatkan akses data-data yang terdapat [20]. Adapun jenis-jenis percobaan yang dilakukan oleh seorang peretas pada sebuah sistem yaitu:

1. *Vulnerability Testing*

   Vulnerability atau kerentanan menurut Janner Simarmata (2006) adalah suatu kelemahan yang terdapat pada suatu aset

sehingga kelemahan tersebut dapat dimanfaatkan oleh oknum yang tidak bertanggung jawab seperti peretas dimana aset tersebut memiliki suatu nilai terhadap suatu perusahaan [21]. Sehingga dapat disimpulkan bahwa *testing* ini berfungsi untuk mencari kelemahan atau kerentanan tersebut sehingga aset akan tetap aman dari peretas yang tidak bertanggung jawab.

2. *Penetration Testing*

Penetration testing lebih mengarah pada berbagai macam penyerangan yang memiliki potensi kelemahan seperti penyerangan server, aplikasi web, piranti mobile dan potensi kelemahan yang lainnya. Berdasarkan modul CEH (*Certified Ethical Hacking*), *penetration testing* merupakan metode mengevaluasi sistem keamanan yang dimiliki oleh suatu sistem dengan cara memberikan serangan dengan tujuan mengetahui serangan apa saja yang dapat melewati keamanan sistem tersebut [22]. Sedangkan menurut Engebretson dan Patrick (2011), *penetration testing* adalah pengeksplotasian keamanan sistem komputer secara sah guna membuat sistem tersebut menjadi lebih aman dengan memperbaiki kelemahan-kelemahan tersebut selama pengujian [23].

3. *Black Box Testing*

Menurut Rizky (2011) *blackbox testing* merupakan suatu pengujian perangkat lunak dimana penguji tidak mengetahui kinerja internal perangkat lunak tersebut [24]. Sehingga dapat dibilang bahwa pada *blackbox testing* penguji memposisikan diri mereka sebagai peretas karena penguji tidak dibekali informasi apapun mengenai sistem yang akan mereka uji keamanannya.

3.5. Keamanan Sistem Informasi

Keamanan Sistem Informasi merupakan suatu cara dimana seseorang dapat mencegah terjadinya pengambilan informasi secara tidak legal yang dilakukan oleh oknum yang tidak bertanggung jawab. Menurut G. J. Simons (2000) adalah bagaimana cara user atau pengguna dapat mencegah atau paling tidak mendeteksi terjadinya penipuan pada sebuah sistem informasi dimana informasi tersebut tidak memiliki arti fisik [25]. Terdapat juga prinsip-prinsip dasar yang harus dimiliki keamanan sistem

informasi yaitu kerahasiaan (*confidentiality)*, ketersediaan (*availability*) dan integritas (*integrity*).

3.6. Framework

Framework merupakan sebuah kerangka kerja yang dapat digunakan sehingga proses pengerjaan menjadi lebih terstruktur. *Framework* dapat dibilang sebagai panduan atau arahan terstruktur kepada pengguna untuk memecahkan suatu masalah. Menurut Daqiqil (2011) *framework* adalah sebuah struktur konseptual dasar digunakan untuk menyelesaikan permasalahan atau isu yang kompleks [26]. Adapun juga beberapa *framework* yang digunakan untuk menguji keamanan sistem:

1. ISSAF

   Framework ISSAF (*The Information System Security Assessment Framework*) merupakan metodologi uji penetrasi yang digunakan untuk mengevaluasi jaringan, kontrol dan sistem sebuah aplikasi [27]. *Framework* ISSAF menawarkan tahapan-tahapan uji penetrasi secara optimal sehingga pengujian dapat terlaksana secara lengkap dan benar dalam pengujian serangan yang sifatnya acak [28]. Terdapat tiga macam langkah kerangka kerja ISSAF yaitu persiapan dan perancangan, pengujian, dan pelaporan dan pembersihan jejak.

2. NIST

   NIST (*National Institute of Standards and Technology*) merupakan sebuah *framework* keamanan sistem yang bertujuan untuk mencegah, mendeteksi, merespon suatu organisasi dalam serangan siber [29]. Pada *framework* NIST terdapat 5 fungsi inti yang menjadi gambaran umum tentang organisasi keamanan siber yaitu: i*dentification* (identifikasi), *protect* (perlindungan), d*etection* (deteksi), *respond* (tanggapan) dan *recover* (pemulihan) [29].

3. OWASP

   OWASP (*Open Web Application Security Project*) merupakan sebuah *framework* yang dibangun dengan tujuan untuk

mencari suatu kelemahan atau celah terhadap suatu aplikasi website [30]. Berdasarkan standar OWASP terdapat sebelas langkah yang terdapat untuk menilai dan menguji keamanan sebuah aplikasi website yaitu: *information gathering*, *configuration management*, *secure transmission*, *authentication*, *session management*, *authorization*, *cryptography*, *data validation*, *denial of service* dan *error handling*.

3.7. Whois

Whois merupakan sebuah *query* yang dapat digunakan untuk mendapatkan sebuah informasi pada domain. Informasi yang dapat diambil oleh whois bermacam-macam mulai dari nama domain, id domain, tanggal kadaluarsa domain, kapan didaftar, *email* dan nomor telepon. Mendapatkan informasi mengenai suatu domain merupakan tugas dari whois. Akan tetapi whois hanya dapat memberikan informasi umum terhadap suatu domain saja [31].

3.8. Spiderfoot

Spiderfoot merupakan perangkat *open source* yang dapat dipakai untuk melakukan pemindaian dan analisis jaringan terhadap suatu situs. Terdapat berbagai macam pengaturan konfigurasi yang ada pada spiderfoot, salah satunya adalah pemindaian dengan menggunakan kasus. Pada opsi pemindaian ini, penguji dapat memilih antara ingin melakukan pemindaian secara aktif maupun pasif terhadap target [32].

3.9. WhatWeb

WhatWeb merupakan sebuah alat yang dapat menemukan kerentanan pada *website*. Whatweb menawarkan dua macam pemindaian yaitu pemindaian pasif dan agresif. Pemindaian pasif hanya mengextrak data-data dari *header* HTTP, sedangkan pemindaian agresif menggunakan berbagai macam *query* dan dapat mengindentifikasi teknologi dibalik *website* sama seperti *vulnerability scanner* yang lainnya [33].

3.10. NMAP

Network Mapper atau NMAP merupakan alat yang dapat melakukan pemindaian *port* terhadap suatu jaringan dan juga dapat memeriksa sebuah jaringan. Untuk memeriksa sebuah jaringan, Nmap bekerja dengan cara menggunakan IP target agar dapat mengetahui nama dan versi dari perangkat lunak yang digunakan target, sistem operasi, dan jenis *firewall* yang digunakan. Selanjutnya Nmap juga dapat melakukan pemindaian terhadap *port* sebuah jaringan sehingga penguji dapat mengetahui *port* berapa yang rentan sehingga dapat melakukan serangan-serangan berdasarkan kelemahan tersebut [34].

3.11. Nessus

Nessus merupakan aplikasi dari Tenable Security yang dapat melakukan *vulnerability scan*. Nessus juga gratis bagi kegunaan *non-enterprise* dan dapat digunakan di berbagai macam sistem operasi seperti Windows, Mac dan Linux. Nessus memiliki *template* pemindaian yang dapat digunakan penguji, seperti *Basic Scan, Discovery, Assessment, Report, Advanced Scan* dan yang lainnya. Nessus juga dapat menggali informasi yang lebih lagi mengenai suatu kerentanan dan sebuah host yang spesifik [35].

3.12. Burp Suite

Burp Suite menggunakan peneliti terkemuka dunia milik PortSwigger untuk membantu pengguna menemukan kerentanan dengan jangkauan yang lebar pada sebuah situs.Burp Suite merupakan sebuah alat yang dapat digunakan untuk melakukan *automated scan* terhadap sebuah situs untuk menemukan konten dan audit untuk sebuah celah atau kerentanan. Terdapat dua tahap *scan* utama pada burp scan yaitu *crawling* dan *auditing*. *Crawling* merupakan kegiatan navigasi terhadap target, mengikuti link, melakukan login Ketika diperlukan guna membuat katalog konten dan jalur navigasi didalamnya. Sedangkan *auditing* merupakan kegiatan analisis jaringan dan tingkah laku target guna mencari kerentanan dan isu lainnya [36].

3.13. Metasploit

Metasploit merupakan alat *open source* yang dapat digunakan untuk menyelidiki kerentanan yang terdapat pada suatu jaringan dan server. Karena bersifat *open source*, Metasploit dapat dengan mudah dimodifikasi dan digunakan pada berbagai macam sistem operasi. Sekarang, Metasploit mengandung lebih dari 1677 *exploits* yang diatur 25 *platform* termasuk Android, PHP, Python, Java, Cisco dan yang lainnya. Dengan fleksibilitas yang dimiliki Metasploit, tim keamanan dapat menggunakan modul yang sudah ada atau membuat sendiri untuk menemukan sebuah kelemahan target.