Big Data Analytics for Cybersecurity

Muhammad Azhar Prabukusumo
Magister Ilmu Komputer, Universitas Budi Luhur
Jl. Ciledug Raya, Pesanggrahan, Jakarta Selatan
2011600513@student.budiluhur.ac.id

***Abstrak*— Era *Internet of Things* dengan miliaran perangkat yang terhubung telah menciptakan permukaan yang semakin besar untuk dieksploitasi oleh penyerang dunia maya, yang mengakibatkan kebutuhan akan deteksi serangan tersebut semakin cepat, mutakhir dan akurat. Beberapa tahun terakhir ini pertumbuhan data dalam volume, kebenaran, kecepatan, dan variasi data luar biasa cepat. Ketika kumpulan besar data atau lebih dikenal dengan *Big Data* itu dikumpulkan dari atau dihasilkan oleh perangkat dan sumber yang berbeda, teknik analisis data besar yang cerdas diperlukan untuk menambang, menafsirkan, dan memvisualisasikan data tersebut. Dalam hal pertahanan keamanan sistem informasi belum ada proteksi perlindungan yang bisa menjamin bahwa tidak akan ada sama sekali serangan ataupun tindakan simulasi siber ke dalam suatu perusahaan atau organisasi. Terlebih di dalam undang-undang yang mengatur terhadap perlindungan data pribadi *GDPR (General Data Protection Regulation)* khususnya di Indonesia belum juga tuntas dibahas oleh para pembuat regulasi maka penggunaan alat bantu otomatis dikombinasikan dengan pusat operasi keamanan yang terdiri dari tenaga ahli serta berkolaborasi dengan *global threat intelligence* adalah metode kolaborasi yang paling mutakhir sebagai tindakan pencegahan dan tepat untuk saat ini agar lebih proaktif dan juga sangat berguna untuk mencegah serangan siber. Tujuan dari penelitian ini yaitu memberikan pengetahuan dan pemahaman kekuatan yang dimiliki dan pentingnya penggunaan alat bantu otomatis atau bekerjasama dengan pusat operasi keamanan yang mempunyai standarisasi internasional dalam mengelola *log event* dari semua perangkat IT yang dimiliki di dalam suatu perusahaan atau organisasi agar sistem keamanan informasi terutama kerentanan dari suatu alat bisa dideteksi secara dini terlebih mengenai kebocoran data dapat diminimalisir.**

***Kata Kunci*— *Big Data Analytics, Cyber Security, Threat Intelligence, Attack Surface, Security Operations Center*.**

***Abstract*-- The era of the Internet of Things with billions of connected devices has created an increasingly large surface for cyber attackers to exploit, resulting in the need for faster, up-to-date and accurate detection of such attacks. The last few years the growth of data in volume, correctness, speed, and variation of data is extremely fast. When large data sets or better known as Big Data are collected from or generated by different devices and sources, intelligent big data analysis techniques are required to mine, interpret and visualize the data. In terms of information system security, there is no protection that can guarantee that there will be no attacks or cyber simulation actions against a company or organization. Moreover, the laws governing the protection of personal data GDPR (General Data Protection Regulation), especially in Indonesia, have not been thoroughly discussed by regulators, so the use of automated tools is combined with a security operations center consisting of experts and collaborating with global threats. intelligence is the most up-to-date collaborative method as a precautionary measure and right now to be more proactive and also very useful for preventing cyber attacks. The purpose of this research is to provide knowledge and understanding of the strengths and the importance of using automated tools or collaborating with security operations centers that have international standards in managing event logs of all IT devices owned within a company or organization so that information security systems, especially vulnerabilities from a tool can be detected early, especially regarding data leakage can be minimized.**

***Kata Kunci*— *Big Data Analytics, Cyber Security, Threat Intelligence, Attack Surface, Security Operations Center*.**

I. PENDAHULUAN

Dengan meningkatnya volume data, termasuk informasi sensitif dan pribadi yang disimpan di layanan online terdistribusi seperti *cloud*, pelanggaran data dan kebocoran privasi adalah masalah yang mendesak dan menantang[1]. Transformasi digital adalah bagaimana suatu perusahaan atau organisasi bisa dengan cepat beradaptasi dan memanfaatkan teknologi informasi. Pengujian Perangkat Lunak dianggap sebagai salah satu fase penting dalam pengembangan perangkat lunak apa pun yang digunakan untuk memastikan kualitas produk perangkat lunak. Dalam setiap siklus hidup pengembangan perangkat lunak *(SDLC)*, fase pengujian perangkat lunak dianggap penting. Pada saat yang sama, dikatakan bahwa 50% dari total biaya pengembangan perangkat lunak dihabiskan untuk fase pengujian perangkat lunak[2]. Pertahanan keamanan sistem informasi perlu diterapkan dan selalu diperbaharui agar akses informasi dan kerahasiaan data tetap terjaga dengan baik.

Perusahaan besar menghasilkan sekitar 10 hingga 100 miliar peristiwa per hari, tergantung pada ukurannya[3]. Jumlah ini hanya akan bertambah karena perusahaan mengaktifkan pencatatan peristiwa di lebih banyak sumber, mempekerjakan lebih banyak karyawan, menyebarkan lebih banyak perangkat, dan menjalankan lebih banyak perangkat lunak. Sehingga volume dan variasi data ini dengan cepat menjadi luar biasa.

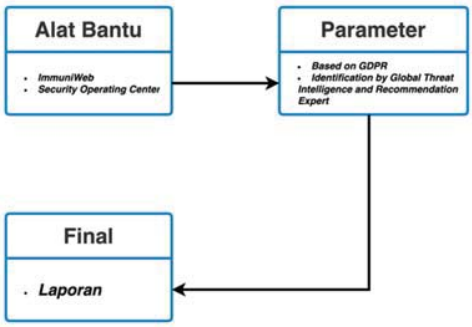
Belum lagi kami menggunakan jejak tumpukan *dump crash* untuk memperkirakan permukaan serangan *Mozilla Firefox*. Kami kemudian menghasilkan kumpulan data dari 271 file rentan di *Firefox*, yang diklasifikasikan menggunakan sistem *Common Weakness Enumeration (CWE)*[4] serangan permukaan yang dilakukan oleh pihak eksternal yang mencoba untuk mengumpulkan informasi berupa kerentanan dari aplikasi website, kelemahan sebuah kata kunci, *miss configuration* pada perangkat keamanan yang digunakan.

Kekuatan analitik data besar begitu hebat sehingga selain semua kemungkinan bisnis, ada banyak masalah privasi baru

yang sedang dibuat[5]. Teknik analitik yang ada tidak bekerja dengan baik pada skala besar dan biasanya menghasilkan begitu banyak kesalahan positif. Masalahnya menjadi lebih kompleks ketika perusahaan pindah ke arsitektur cloud dan mengumpulkan lebih banyak data. Maka diperlukan sebuah tindakan terukur agar tidak terjadi kebocoran data yang bisa mengakibatkan nilai sebuah perusahaan atau organisasi menurun terlebih tidak mendapatkan kepercayaan lagi oleh pelanggan.

II. METODOLOGI

Tes penetrasi dan pemindaian kerentanan otomatis saat ini semakin banyak digunakan untuk mendeteksi kelemahan selama pengoperasian sistem TI jaringan. Analisis kerentanan dijalankan untuk menemukan kerentanan dalam sistem yang dapat dieksploitasi oleh penguji penetrasi[6]. Metode yang digunakan dalam penelitian ini adalah metode eksperimental dan studi pustaka. Penelitian dimulai dengan studi dokumen yang diperoleh dari buku, *e-book* dan materi terkait penelitian[7] kemudian eksperimen dilakukan dengan pemilihan alat otomatis untuk pengujian keamanan dan kombinasi pusat operasi keamanan yang terdiri dari tenaga ahli berkolaborasi dengan *global threat intelligence*, penelitian ini mengadopsi pendekatan melakukan pengujian keamanan pada aplikasi website tertentu yang dipilih untuk pengujian. Proses ini dilakukan secara bertahap, mulai dari pemilihan alat bantu untuk identifikasi aplikasi website universitas swasta. Memilih kategori kunci dalam metodologi yang diadopsi yaitu memilih alat otomatis untuk pengujian, mengidentifikasi aplikasi website universitas swasta untuk pengujian, melaksanakan pengujian, menginterpretasikan hasil, dan membandingkannya. Selain itu mengkombinasikan alat otomatis dengan tenaga ahli dan *global threat intelligence* yang dapat memberikan analisa terukur dan valid.



Gbr. 1 Terminologi untuk *Cyber Security*

III. HASIL DAN PEMBAHASAN

ImmuniWeb adalah *Application Cloud Platform Security* yang berdiri tahun 2014 dan berasal dari Swiss, meraih banyak penghargaan diantaranya *SC Award 2018* untuk kategori *best usage of Machine Learning and Artificial Intelligence. Machine Learning* yang diterapkan oleh ImmuniWeb sangat sudah teruji dengan diinfokan di halaman web utama nya yaitu lebih dari 220 Juta test yang sudah menggunakan alat bantu otomatis ini. Selain itu *Immune Web* sudah memiliki ISO 27001;2013 dan *Crest Accredited* untuk *Penetration Test*. Dari 4 modul yang dimiliki Immune Web yaitu:

1. ***Immune Web Discovery***
   Dark Web and Attack Surface Monitoring (Annual subscription-12 Month)
2. ***Immune Web On-Demand***
   Web Application Penetration Testing (One time purchase/testing-90 days period guarantee)
3. ***Immune Web Mobile Suite***
   Mobile Application Penetration Testing (Annual subscription-12 Month)
4. ***Immune Web Continuous***
   Continuous Penetration Testing (Annual subscription-12 Month)

Tidak hanya itu *Immune Web* sebagai *Platform Application Cloud Security* juga memberikan *free trial* bagi semua pelanggan di Indonesia yang ingin mencoba beberapa fitur yang ada di *Immune Web* seperti *Immune Web Discovery* dan *Immune Web On-Demand*. Jika fokus pada penetration test bisa menggunakan *ImmuniWeb On-Demand* fitur ini kolaborasi antara *Machine Learning dan Human* sehingga hasil yang didapatkan mendapatkan garansi "*zero false positive*".

ImmuniWeb On-Demand ini diimplementasikan terhadap beberapa aplikasi website dan *mobile phone* yang di dalam fitur ini bisa mendeteksi beberapa kerentanan sesuai standar *OWASP (Open Web Application Security Protection), PCI-DSS, HIPAA dan ISO 27001;2013* untuk website dan *untuk mobile phone* nya fitur ini bisa mendeteksi jika suatu *native* aplikasi yang dikembangkan di *mobile* phone ada suatu kerentanan bahkan *phone* yang sudah di *jailbreak* pun bisa terdeteksi dengan baik.

Metodologi yang akan dilakukan yaitu *vulnerability scanning* adalah kegiatan proses memperoleh informasi *vulnerability network* dengan memanfaatkan berbagai *tools network scanning* dan *vulnerability scanner*, seperti port yang terbuka , bugs aplikasi dan mengetahui serangan serangan yang akan terjadi terhadap kerentanan website yang ada yang akan berdampak cukup buruk[8] apabila terjadi pada aplikasi website universitas swasta. Testing dari sisi *GDPR (General Data Protection Regulation)*, sekilas mengenai *GDPR* yaitu peraturan mengenai perlindungan data (*data privacy*) di mana data pribadi pengguna tidak boleh dimanfaatkan dalam bentuk apapun tanpa seizin pemilik.

Tabel 1. Hasil penilaian by *Immune Web*

Security Analysis	UBL	STI&K	Nusa Mandiri	Mercubuana	Binus
Software Security Test (No of Issues found)	*None*	*None*	*None*	2	*None*

Security Analysis	UBL	STI&K	Nusa Mandiri	Mercubuana	Binus
GDPR Security Analysis (No of Issues found)	1	3	1	4	*None*
PCI DSS Security Analysis (No of Issues found)	1	1	*None*	3	1
HTTP Headers Security Analysis (No of Issues found)	*None*	*None*	5	*None*	*None*
Content Security Policy Security Analysis (If available)	*Missing*	*Missing*	*Missing*	*Missing*	5
Final Score	C+	C+	C+	F	C

Dari hasil diatas bahwa yang menerapkan metode kepatuhan *GDPR* adalah Universitas Binus dengan tidak ditemukannya celah kerentanan mengenai kebocoran data.

Pusat Operasi Keamanan

Secara tradisional, tim pusat operasi jaringan dan keamanan telah bekerja dalam ruang lingkup yang begitu kompleks dan rumit meskipun ada kesamaan. Tim *network operating center (NOC)* bertugas untuk menyediakan operasionalisasi dan ketersediaan aset teknologi informasi (TI), sedangkan *security operation center (SOC)* adalah untuk memastikan keamanan aset TI dan melindunginya dari serangan keamanan siber[9]. *Security Operation Center (SOC)* adalah fasilitas yang terdiri dari komponen penting dalam mendukung keamanan jaringan atau *IT security* suatu perusahaan. Sasarannya, *SOC* untuk mendeteksi, menganalisis, dan menanggapi insiden keamanan siber dengan menggunakan kombinasi solusi teknologi dan serangkaian proses. *SOC* penting karena mendukung keamanan TI, layanan yang diberikan adalah dengan perjanjian tingkat layanan yaitu 24 Jam x 7 hari dalam seminggu x 365 hari dalam satu tahun melindungi keamanan organisasi/perusahaan, dan menjaga integritas bisnis anda agar memenuhi standar layanan bahkan berkembang tanpa khawatir akan ancaman kejahatan siber.

SOC mempunyai terminologi yaitu;

1. *People*
   - *Staff Training and Awareness*
   - *Professional Skills and Qualification*
   - *Competent Resources*
2. Proses
   - *Management Systems*
   - *Governance Frameworks*
   - *Best Practice*
   - *IT Audit*
3. Teknologi
   - Belum bisa mengimplementasikan teknologi tanpa orang yang mempunyai kompetensi di bidangnya untuk mendukung proses atau rencana keseluruhan

Apa itu *Threat Intelligence*?

Threat Intelligence adalah pendekatan keamanan siber yang dilakukan dengan cara mengumpulkan, memproses, dan menganalisa data untuk memahami motif, target, dan perilaku penjahat siber. *Threat Intelligence* memungkinkan tim keamanan IT untuk membuat keputusan keamanan yang lebih cepat dan terinformasi, mengubah tindakan yang dapat dilakukan untuk melindungi sistem keamanan yang awalnya hanya sekedar tindakan reaktif menjadi tindakan proaktif. Jadi, pendekatan *Threat Intelligence* yang didasari oleh data akan menjadi acuan untuk mengambil tindakan atau keputusan atas ancaman siber yang terjadi.

Apa yang menjadikan *Threat Intelligence penting bagi perusahaan*?

Threat Intelligence penting bagi perusahaan karena seperti yang sudah disebutkan sebelumnya, *Threat Intelligence* membantu tim keamanan IT untuk memahami motif, target, serta pola perilaku penjahat siber yang mencakup taktik atau teknik, dan prosedur yang mereka gunakan *(HTTPs).*

Dengan data dan informasi yang tersedia tersebut, tim keamanan IT mampu memahami aspek-aspek yang sebelumnya tidak dapat diketahui, sehingga mereka dapat membuat keputusan yang lebih tepat pada saat terjadi penyerangan pada sistem perusahaan.

Jadi, dapat disimpulkan bahwa *Threat Intelligence* memberikan gambaran utuh yang membuat tim keamanan IT bisa mengambil kesimpulan tepat berdasarkan semua informasi yang ada atau yang dikenal sebagai *data-driven decisions*.

Di *SOC* dengan kombinasi *Global Threat Intelligence* dan tenaga ahli keamanan informasi sehingga incident alarm dapat dianalisa, dibuktikan dan valid sehingga tidak terjadi kesalahan dalam laporan, peran teknologi juga tidak kalah penting yaitu diantaranya penggunaan *SIEM (Security Incident and Event Monitoring),* Sekilas mengenai *SIEM* yaitu singkatan dari informasi keamanan "sim" dan manajemen event "sem" dan diucapkan *"SIEM"*. Ini adalah sistem yang mengumpulkan file log, peringatan keamanan, dan peristiwa ke dalam satu tempat, sehingga tim keamanan dapat menganalisis data dengan lebih mudah. Anda dapat menganggap *SIEM* sebagai sistem manajemen log khusus untuk keamanan. *SIEM* mengumpulkan

semua informasi ini dari sistem keamanan lain seperti keamanan titik akhir, *firewall,* sistem deteksi intrusi, dan sejenisnya. Mereka diperlukan dengan pertumbuhan jumlah sistem keamanan.

SOC dalam *managed service* dan digunakan oleh suatu perusahaan atau organisasi untuk menjaga keamanan sistem yang sudah dibangun maupun sebagai tindakan pencegahan dan perencanaan yang lebih terukur dan valid. *Next Generation SIEM* sudah menggunakan teknologi *UEBA (User and Entity Behaviour Analytics)* yang bertugas menganalisis perilaku pengguna

Penjelasan singkat mengenai *UEBA*

Anomali dalam akses jaringan membuat arus lalu lintas yang tidak diinginkan di jaringan organisasi. Mereka termasuk akses tidak sah oleh pengguna seperti alamat *IP* milik satu perusahaan yang digunakan oleh karyawan perusahaan lain atau mengakses *IP* organisasi dari luar jaringan atau lokasi perusahaan. Mereka menimbulkan ancaman terhadap integritas data dan dapat mengakibatkan data bisnis terekspos ke jaringan pihak ketiga. Beberapa pengguna yang memiliki akses jarak jauh, terhubung ke jaringan kantor dari jaringan pribadi mereka saat bepergian atau bekerja dari rumah. Meskipun keluar dari organisasi, beberapa pengguna masih dapat mengakses jaringan perusahaan jika akses mereka tidak dicabut dengan benar. Makalah ini melalui pendekatan *UEBA*, berfokus pada pemantauan profil pengguna, data penggunaan jaringan mereka, *Alamat IP*, Lokasi Akses dan Perusahaan tempat pengguna berada, selama periode waktu tertentu dan mengklasifikasikannya ke dalam penggunaan normal dan anomali. Para peneliti menggunakan metode analisis visualisasi data untuk membuat representasi visual data untuk dianalisis dan mendeteksi anomali di dalamnya.

berikutnya *SOAR (Security Orchestration Automation and Response)* yang bertugas untuk mengkonsolidasi semua perangkat *security* dalam satu management sehingga jika terjadi incident dapat ditutup dulu dengan cepat agar tidak menyebar ke perangkat yang lain.
Manage Service itu dibagi menjadi beberapa tingkatan diantaranya;

1. ***Tier 1-Alert Analyst***
   Di tingkatan Tier 1 ini diisi oleh seorang analis keamanan siber atau rekanan yang mempunyai tugas melacak notifikasi serangan yang masuk, verifikasi dan memastikan bahwa telah terjadi serangan lalu eskalasi ke Tier 2
2. ***Tier 2-Incident Responder***
   Para ahli ini bertanggung jawab untuk melakukan investigasi mendalam terhadap insiden dan merekomendasikan perbaikan atau intervensi.
3. ***Tier 3-Threat Hunter***
   Para ahli ini memiliki pengetahuan tingkat lanjut tentang jaringan, titik akhir, *intelijen* ancaman, dan *malware* rekayasa terbalik. Mereka ahli dalam melacak proses malware untuk menilai efeknya dan cara menghapusnya. Mereka juga sangat terlibat dalam pencarian ancaman baru dan penyebaran perangkat lunak pendeteksi ancaman. Pemburu ancaman mencari ancaman dunia maya yang belum diidentifikasi tetapi ada dalam jaringan.
4. ***SOC Manager***
   Individu ini bertanggung jawab atas sumber daya *SOC* dan bertindak sebagai titik kontak dengan perusahaan yang lebih besar atau pelanggan.

Pada dasarnya, semua *Next Generation SIEM* memiliki kapasitas untuk mengumpulkan, menyimpan, dan menghubungkan peristiwa dihasilkan oleh infrastruktur yang dikelola[10].

Beberapa produk *SIEM* yang ada di pasar dan sudah digunakan oleh beberapa pusat operasi keamanan diantaranya;

1. *ArcSight*
2. *QRadar*
3. *McAfee*
4. *LogRhythm*
5. *RSA dan*
6. *Splunk*

Dari keenam produk *SIEM* diatas yang belum mendukung fitur *UEBA* adalah *McAfee* kemungkinan kedepannya *McAfee* bisa mengembangkan atau bisa bekerjasama dengan *vendor atau produk UEBA* yang sudah memiliki dasar pelanggan yang luas dan fitur yang kuat.

Pusat Operasi Keamanan membutuhkan satu manajemen kesatuan untuk monitor semua *anomali traffic IP address* yang kemungkinan dicurigai sebagai *ransomware* sebagai contoh dilihat dari intensitas *three-way handshake* nya.
Berikut tahap-tahap nya:

1. Kita ambil contoh ip address yang dicurigai yaitu 149.56.24.226 (*IP Address* ini adalah website film apapun dengan bebas akses dan *download* gratis.
2. Setelah itu sebagai analis sistem keamanan harus memastikan bahwa *ip address* tersebut benar mengandung *malicious* atau tidak yaitu dengan cara akses *https://www.virustotal.com/gui/home/search*
3. Masukkan *IP address* yang dicurigai dan klik search di website tersebut dan muncul satu *suspicious.*

Penetration Testing

Penetration Test merupakan salah satu upaya untuk meningkatkan dan menguji kualitas aplikasi, infrastruktur dan sistem dalam menunjang proses bisnis Perusahaan yang menggunakan layanan TI. Beberapa studi literatur yang menggunakan Jasa *Penetration Test* terhadap Jaringan Infrastruktur diantaranya;

1. Menurut penelitian yang dilakukan oleh [11] *testing* terhadap *wireless* PT. Puma Makmur Aneka Engineering. Dari hasil analisis yang telah dilakukan, didapatkan kesimpulan bahwa jaringan wireless pada PT. Puma Makmur Aneka Engineering tidak aman karena masih ada titik *hotspot* yang dapat dilakukan *crack.*

2. Menurut penelitian yang dilakukan oleh [12] bahwa sistem keamanan jaringan yang terdapat pada sistem *pay2home* pada bagian namun pada bagian website masih terdapat celah, pada bagian *port service* terdapat *service* yang terbuka sehingga memungkinan terjadinya penyerangan, Sistem keamanan jaringan yang baru dapat dicapai dengan mematikan *service port* serta menggunakan perintah *Deny*.

Dengan dua studi literatur diatas membuktikan *penetration test* tidak dilakukan secara keseluruhan atau hanya dari satu sisi sehingga belum bisa diambil kesimpulannya. Maka dari itu dengan adanya *Penetration Test* kombinasi antara ImmuniWeb dan *Human* diharapkan pelanggan dapat mengetahui kelemahan dan kerentanan secara keseluruhan yang terdapat dalam aplikasi dan infrastruktur dari sudut pandang hacker serta *comply* terhadap peraturan atau regulasi yang mengatur sistem distribusi dan manufaktur. Adanya serangan keamanan yang dilakukan oleh *hacker* bisa berdampak pada aplikasi dan ketersediaan data yang berimplikasi terganggunya operasi bisnis selain itu bisa berdampak pada image perusahaan apabila sampai terjadi kebocoran data penting, pendekatan *penetration test* dilakukan dengan cara:

1. ***Black Box Testing***

   Pada pengujian dengan jenis *Black Box* testing, *pentester* hanya akan diberikan *IP* target yang akan dilakukan *Penetration Test*. Tujuan dari *black box* testing ini untuk memberikan gambaran serangan dari lingkungan external. Dengan melakukan *black box* testing ini, hasil yang diharapkan adalah sebuah analisis serangan dari external.

   - Batasan pekerjaan *Black Box Testing*

     Penetration *Test* dilakukan dalam kondisi *Black Box testing* dimana *Pentester* diberikan IP target dalam pelaksanaan *Penetration Test*. Secara spesifik, metode *black box* testing yang dilakukan dalam pelaksanaan pekerjaan *Penetration Test* di client dengan dilakukannya melalui jaringan eksternal. Kondisi *Penetration Test* ini mensimulasikan situasi layaknya *hacker* (penyerang) yang belum mengetahui atau memiliki akses kedalam sistem jaringan internal kantor client dan mencoba mencari kerentanan terhadap sistem client.

2. ***Grey Box Testing***

   Pada pengujian dengan jenis *Grey Box* testing, Penetration tester hanya akan diberikan informasi yang terbatas terkait target yang akan di *Penetration Test*. Tujuan dari *Grey Box* testing ini untuk memberikan gambaran serangan dari lingkungan external dan internal. *Pentester* akan bertindak sebagai user karyawan dan bisa seperti orang lain yang belum mengetahui *flow (alur)* dari aplikasi.

   - Batasan pekerjaan *Grey Box Testing*

     Penetration *Test* dilakukan dalam kondisi *Black Box testing* dimana *Pentester* diberikan IP target dalam pelaksanaan *Penetration Test*. Secara spesifik, metode *black box* testing yang dilakukan dalam pelaksanaan pekerjaan *Penetration Test* di client dengan dilakukannya melalui jaringan eksternal. Kondisi *Penetration Test* ini mensimulasikan situasi layaknya *hacker* (penyerang) yang belum mengetahui atau memiliki akses kedalam sistem jaringan internal kantor client dan mencoba mencari kerentanan terhadap sistem client.

3. ***White Box Testing***

   Metode *penetration testing white box* dilakukan ketika perusahaan ingin mendeteksi kerentanan sekecil apapun di dalam system atau aplikasi. Hal ini yang membuat pengujian dengan metode *white box* membutuhkan waktu yang cukup lama.

   - Batasan pekerjaan *White Box Testing*

     Dalam proses testing, penguji harus diberikan akses ke semua informasi yang dibutuhkan termasuk *source code* dan *flow* aplikasi. Hal ini membuat penguji dapat memeriksa sistem secara menyeluruh dan mencapai tahap yang mungkin belum dapat terakses dengan metode *black box* atau *grey box*.

Tabel 2. Tahapan Pekerjaan *Penetration Testing*

Fase	Deskripsi	Aktifitas
Planning	Tahapan *planning* dilakukan untuk mendapatkan detail pekerjaan dan menentukan kebutuhan setiap *stakeholder*	● Memahami konteks bisnis dan flow aplikasi ● Mendefinisikan ruang lingkup pekerjaan ● menyiapkan segala kebutuhan *pentest* dan *timeline*
Assessment	Proses *pentest* yang dilakukan untuk mengevaluasi tingkat keamanan pada sebuah sistem. Proses dilakukan dengan cara manual maupun menggunakan alat bantu otomatis	● *Information gathering* ● *Perform assessment* ● Menginformasikan pelanggan jika ditemukan *risk* yang *critical*
Reporting	Menyediakan dokumen untuk memaparkan dan mengklarifikasi setiap temuan dengan rekomendasi perbaikan	● Verifikasi temuan ● *Submit report* ● Menyediakan rekomendasi untuk perbaikan setiap temuan
Re-test	Memverifikasi hasil perbaikan berdasarkan rekomendasi yang diberikan di dalam laporan temuan	● *Follow up* dan memverifikasi remediasi setiap temuan ● menyelesaikan proses assessment
Final report	Memberikan laporan berupa dokumentasi lengkap mulai dari *planning* sampai dengan *re-test*	Memberikan final dokumen berupa mitigasi dan hasil serta perbaikan-perbaikan yang sudah dilakukan..

IV. KESIMPULAN

Hasil pengujian yang dihasilkan oleh *ImmuniWeb* diantaranya yaitu :

1. Interaktif dan mudah dipahami hasil yang ditampilkan oleh *ImmuniWeb*
2. *ImmuniWeb* bisa diintegrasikan dengan beberapa perangkat security seperti Imperva, Fortinet, F5, Splunk dan tidak hanya itu *ImmuniWeb* sudah bekerjasama dengan beberapa *vendor cloud* dan beberapa *vendor open software*.
3. *Zero False Positive* karena kombinasi antara *machine learning* dengan *expert human yang ditawarkan oleh alat bantu otomatis ini* serta
4. *Security Operating Center* sangat membantu dalam hal menganalisa data yang begitu besar dengan waktu yang cepat dan valid. Maka dari itu tindakan pencegahan dan proaktif sangat dibutuhkan di era digital yang begitu cepat dan adaptif sehingga serangan siber dapat diminimalisir.

KONFLIK KEPENTINGAN (WAJIB)

Benar adanya bahwa penulis menyatakan bahwa tulisan ini tidak ada konflik kepentingan dengan siapapun dan murni hasil dari penelitian yang ditujukkan untuk kepentingan publikasi meraih gelar Magister Ilmu Komputer.

REFERENSI

[1] A. Azmoodeh dan A. Dehghantanha, “Big Data and Privacy: Challenges and Opportunities BT - Handbook of Big Data Privacy,” K.-K. R. Choo dan A. Dehghantanha, Ed. Cham: Springer International Publishing, 2020, hal. 1–5.

[2] M. M. F. Naja, A. R. F. Shafana, dan A. F. Musfira, “Automated Software Testing and Tool Selection : Case Study Based on Security Testing of Popular E-commerce Applications in Malaysia,” no. Icst, 2021.

[3] A. A. Cardenas, P. K. Manadhata, dan S. P. Rajan, “Big data analytics for security,” *IEEE Secur. Priv.*, vol. 11, no. 6, hal. 74–76, 2013.

[4] C. Theisen, H. Sohn, D. Tripp, dan L. Williams, “BP: Profiling Vulnerabilities on the Attack Surface,” in *2018 IEEE Cybersecurity Development (SecDev)*, 2018, hal. 110–119, doi: 10.1109/SecDev.2018.00022.

[5] A. D. Mishra dan Y. B. Singh, “Big data analytics for security and privacy challenges,” in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, hal. 50–53.

[6] Y. Mahmoodi, S. Reiter, A. Viehl, O. Bringmann, dan W. Rosenstiel, “Attack Surface Modeling and Assessment for Penetration Testing of IoT System Designs,” in *2018 21st Euromicro Conference on Digital System Design (DSD)*, 2018, hal. 177–181, doi: 10.1109/DSD.2018.00043.

[7] R. Pamungkas dan F. W. Z. Zaney, “Penerapan Hashing SHA1 dan Algoritma Asimetris RSA untuk Keamanan Data pada Sistem Informasi berbasis Web,” *Res. J. Comput. Inf. Syst. Technol. Manga.*, vol. 4, no. 1, hal. 84–89, 2021.

[8] M. Fatkhurozi, “Analisa Keamanan Website Menggunakan Metode Footprinting dan Vulnerability Scanning pada Website Kampus,” in *Prosiding Seminar Nasional Informatika Bela Negara*, 2021, vol. 2, hal. 144–148.

[9] D. Shahjee dan N. Ware, “Integrated Network and Security Operation Center: A Systematic Analysis (February 2022),” *IEEE Access*, hal. 1, 2022, doi: 10.1109/ACCESS.2022.3157738.

[10] G. González-Granadillo, S. González-Zarzosa, dan R. Diaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,” *Sensors* , vol. 21, no. 14. 2021, doi: 10.3390/s21144759.

[11] R. W. Ismail dan R. Pramudita, “Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi,” *J. Mhs. BINA Insa. Vol 5 No 1 J. Mhs. Bina Insa. (Agustus 2020)*, Agu 2020, [Daring]. Tersedia pada: http://ejournal-binainsani.ac.id/index.php/JMBI/article/view/1373.

[12] S. E. Prasetyo dan R. C. Lee, “Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing,” *Comb. - Conf. Manga. Business, Innov. Educ. Soc. Sci. Vol 1 No 1 Conf. Manga. Business, Innov. Educ. Soc. Sci.*, Mar 2021, [Daring]. Tersedia pada: https://journal.uib.ac.id/index.php/combines/article/view/4500.