Jurnal Riset Internasional Teknik dan Teknologi (IRJET) e-ISSN: 2395-0056
Jilid: 07 Edisi: 04 | April 2020 p-ISSN: 2395-0072www.irjet.net

Analisis Tim Merah tentang Tindakan dan Respons Keamanan Informasi

Khushboo Amin1, Dr.Priyanka Sharma2

1 Siswa, Sekolah Teknologi Informasi & Keamanan Siber, Universitas Raksha Shakti, Gujarat, India
2Dekan, Penelitian & Pengembangan, Universitas Raksha Shakti, Gujarat, India

---

Abstrak - *Penelitian ini mencoba untuk mengembangkan pemahaman faktor strategi penilaian Tim Merah dalam keamanan komputer dan data. Tim Merah adalah 'bentuk penilaian berbudaya' yang mengidentifikasi kelemahan dalam sistem informasi dan keamanan yang cukup. Penelitian ini bertujuan untuk mengidentifikasi dan mendefinisikan bentuk dimensi efektivitas Tim Merah dari sisi pelanggan, manajemen, individu, dan anggota tim untuk memperkuat keamanan dan kinerja sistem pengetahuan. Tim Merah umumnya mengatasi risiko perlindungan yang ada dalam sistem pengetahuan melalui Penilaian Kerentanan dan Pengujian Penetrasi (VAPT). VAPT yang terdiri dari dua istilah terpisah yaitu Vulnerability Assessment (VA) dan Penetration Testing (PT) adalah teknik ofensif dimana aset cyber organisasi mana pun dieksploitasi dalam lingkungan terkendali untuk mensimulasikan serangan real-time pada sistem informasi. Penilaian kerentanan mencakup penggunaan berbagai alat otomatis dan teknik pengujian manual untuk menentukan postur perlindungan sistem target. Selama langkah ini, semua titik pelanggaran dan celah ditemukan. Titik/celah pelanggaran ini jika ditemukan oleh penyerang dapat mengakibatkan hilangnya data dalam jumlah besar dan aktivitas intrusi yang menipu. Selama Pengujian Penetrasi, pen-tester menyimulasikan aktivitas yang dilakukan oleh aktor jahat yang mencoba menggunakan kerentanan yang ada dalam sistem yang ditargetkan. Proses VAPT ini membantu dalam menilai efektivitas tindakan perlindungan yang ada pada sistem target.*
Saat menulis makalah ini, saya telah menjelaskan keseluruhan proses VAPT, metodologi, model, dan standar global yang digunakan untuk menilai infrastruktur keamanan informasi.

Kata Kunci: Peretasan etis, Keamanan Informasi, Pengujian Penetrasi, Tim Merah, Pengujian Keamanan, Penilaian Kerentanan.

1. PERKENALAN

Makalah penelitian ini adalah bagian dari proyek saya untuk pemenuhan sebagian untuk mencapai gelar Magister Teknologi. Topik dan konsep yang disebutkan dalam makalah ini dibahas secara menyeluruh dalam laporan proyek beserta kerentanan yang ditemukan dan rekomendasinya.

Seperti yang kita ketahui saat ini, lanskap ancaman keamanan siber bersifat dinamis dan terus berubah. Penyerang dunia maya saat ini menggunakan kombinasi teknik peretasan tradisional dan lanjutan. Selain itu, varian baru dari pelaku ancaman jahat yang ada terlihat setiap hari. Red Teaming adalah simulasi serangan berlapis-lapis dengan cakupan penuh yang dirancang untuk menunjukkan seberapa baik karyawan dan jaringan perusahaan, aplikasi dan kontrol keamanan fisik dapat menahan serangan dari musuh di kehidupan nyata.

2. BERBEDA JENIS TIM

2.1 Tim Merah

Mereka bekerja khusus sebagai bagian dari infrastruktur internal atau entitas eksternal untuk menguji efektivitas mekanisme keamanan dengan meniru alat dan teknik penyerang sedekat serangan di dunia nyata.
infrastruktur.

2.2 Tim Biru

Ini mengacu pada tim keamanan internal yang bekerja sebagai pembela terhadap penyerang internal/eksternal di dunia nyata dan serangan Tim Merah. Tim Biru berbeda dari
tim keamanan tradisional di sebagian besar organisasi, karena sebagian besar personel dalam tim 'operasi keamanan' tidak memiliki mentalitas kewaspadaan terus-menerus terhadap serangan, yang merupakan misi dan perspektif Tim Biru sejati yang menjadikannya bertahan keluar dari operasi keamanan tradisional dan tim pemantauan.

2.3 Tim Ungu

Tim Ungu hadir untuk menegaskan dan memaksimalkan efektivitas tim Merah dan Biru. Itu adalah integrasi taktik bertahan dan kontrol dari Tim Biru dan keterampilan menyerang dari Tim Merah menjadi satu
tim tunggal yang memaksimalkan throughput keamanan. Idealnya, Tim Ungu tidak boleh menjadi sebuah tim sedikit pun, melainkan sebuah dinamika permanen antara Merah dan Biru.

3. PENILAIAN KEAMANAN: VAPT

Penilaian Kerentanan dan Pengujian Penetrasi berada di luar audit dimana celah sistem atau infrastruktur ditemukan secara eksternal.

3.1 Penilaian Kerentanan

Penilaian kerentanan adalah upaya untuk mengidentifikasi, mengklasifikasikan dan memprioritaskan kerentanan yang ditemukan dalam sistem komputer selama penilaian keamanan aplikasi, dan infrastruktur jaringan; memberikan organisasi laporan komprehensif yang membahas status risiko dan dampak bisnis dari setiap kerentanan. Laporan komprehensif ini membantu dalam penilaian yang tepat atas pengetahuan, kesadaran, dan latar belakang risiko yang tersedia untuk memahami ancaman terhadap sistem informasi dari masing-masing kerentanan dan bereaksi sesuai dengan itu.

3.2 Pengujian Penetrasi

Tes penetrasi, juga dikenal sebagai tes pena, mendefinisikan serangan cyber yang disimulasikan terhadap sistem informasi organisasi untuk memeriksa eksploitasi kerentanan. Berbicara dari perspektif keamanan aplikasi web, pengujian penetrasi biasanya digunakan untuk memperkuat firewall aplikasi web (WAF) yang melindungi infrastruktur aplikasi web organisasi.

Pengujian pena berupaya untuk menembus sejumlah sistem aplikasi, titik akhir, dan aset lainnya untuk mengungkap kerentanan yang tersembunyi dalam sistem informasi, seperti memberikan masukan yang rusak sehingga menyebabkan serangan injeksi kode.

4. METODOLOGI

Sebuah sistem metode yang digunakan dalam penilaian kerentanan dan pengujian penetrasi. Tim Merah sangat bergantung pada kebutuhan keamanan klien. Misalnya, seluruh infrastruktur TI dan jaringan mungkin dievaluasi, atau bagian tertentu dari infrastruktur mungkin diuji. Fungsi spesifik dari apa yang akan diuji diperiksa secara kritis berdasarkan hasil evaluasi keamanan.

4.1 Pengintaian

Pengintaian adalah tahap awal; saat penyerang mengumpulkan sebanyak mungkin informasi tentang target dan infrastrukturnya sebelum melancarkan serangan, hal ini membantu penyerang memaksimalkan dampak serangan

4.2 Pemindaian

Fase ini merupakan perpanjangan logis dari pengintaian aktif di mana penyerang menggunakan rincian yang dikumpulkan untuk secara aktif menyelidiki target guna mengidentifikasi titik masuk dan kerentanan yang ada dalam sistem informasi.

4.3 Mendapatkan Akses

Ini adalah fase serangan ketiga dan terpenting dalam hal potensi kerusakan. Akses langsung ke sistem informasi mungkin tidak selalu diperlukan untuk menyebabkan kerusakan. Misalnya, serangan penolakan layanan menghilangkan sumber daya sistem atau menghentikan layanan penting agar tidak berjalan pada sistem target. Sebuah proses pada target dapat dimatikan untuk menghentikan layanan, menggunakan logika/bom waktu, atau bahkan secara sengaja melakukan kesalahan konfigurasi dan membuat sistem crash. Pemadaman jaringan di jaringan lokal dapat menguras sumber daya.

Penyiapan yang ditargetkan dapat dieksploitasi secara lokal di jaringan, offline melalui kontak langsung, atau Internet sebagai sarana penipuan yang menyebabkan pencurian. Banyak faktor yang menyebabkan penyerang berhasil mendapatkan akses ke sistem target seperti arsitektur dan konfigurasi, keahlian penyerang, dan tingkat akses awal yang diperoleh. Jenis serangan penolakan layanan yang paling merusak adalah serangan penolakan layanan terdistribusi, di mana penyerang menggunakan zombie perangkat lunak yang didistribusikan melalui beberapa mesin di Internet untuk memicu penolakan layanan skala besar yang diatur.

4.4 Mempertahankan Akses

Akses Setelah penyerang mendapatkan akses ke sistem target, penyerang dapat memilih untuk menggunakan sistem dan sumber dayanya, dan selanjutnya menggunakan sistem tersebut sebagai poros untuk menembus lebih dalam ke dalam jaringan melalui pemindaian dan eksploitasi sistem lain atau tetap bersikap low profile. disembunyikan untuk terus mengeksploitasi sistem jika diperlukan; kedua tindakan ini sama-sama dapat merusak organisasi dan berdampak pada bisnis dengan cara yang tidak dapat diprediksi. Misalnya, penyerang dapat menggunakan sniffer untuk mengumpulkan lalu lintas yang mengalir di jaringan, termasuk sesi telnet dan FTP yang tidak te

4.5 Membersihkan Jalur

Untuk tetap anonim dan mempertahankan akses sistem, penyerang akan menghancurkan bukti kehadiran dan aktivitasnya. Menghapus bukti adanya kompromi adalah persyaratan bagi penyerang yang ingin tetap tidak dikenal. Ini adalah salah satu metode terbaik untuk menghindari penelusuran kembali.

Hal ini biasanya dimulai dengan menghapus upaya login yang gagal dan pesan kesalahan apa pun yang ditemukan selama fase perolehan akses, misalnya pesan yang tertinggal di log sistem dan penampil peristiwa di sistem Windows. Selanjutnya, tindakannya adalah mengkonfigurasi ulang mekanisme logging untuk menghindari logging upaya login di masa mendatang. Administrator sistem dapat diyakinkan tentang kredibilitas keluaran log sistem yang benar dan tidak ada intrusi atau kompromi sistem dengan memanipulasi dan mengubah log peristiwa.

Risiko = Ancaman * Kerentanan * Dampak

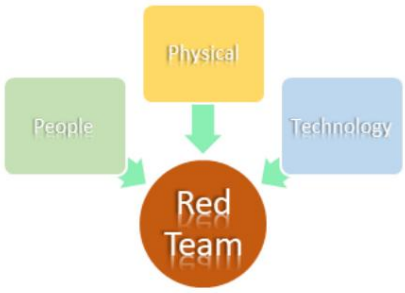
Sesuai SOP, hal pertama yang dilakukan administrator sistem untuk memantau aktivitas yang tidak biasa adalah memeriksa file log sistem, penyusup biasanya menggunakan utilitas untuk mengubah log sistem untuk menghindari administrator. Rootkit dapat digunakan untuk menonaktifkan logging sama sekali dan membuang semua log yang ada sebagai tindakan terbaik yang dilakukan penyusup. Hal ini terjadi jika penyusup berniat menggunakan sistem untuk jangka waktu yang lebih lama sebagai basis peluncuran untuk penyusupan di masa depan. Hanya bagian log yang dapat mengungkap keberadaan penyusup yang kemudian dihapus agar tetap tersembunyi. Sistem harus terlihat dan berfungsi seperti sebelum serangan dan penerapan pintu belakang. Setiap modifikasi pada file kritis/non-kritis harus diubah kembali ke atribut aslinya. Informasi yang tercantum, seperti ukuran file dan tanggal, hanya mengatribusikan informasi yang terdapat di dalam file.

5. TIM MERAH

Ketika digunakan dalam konteks keamanan komputer, Tim Merah adalah sekelompok peretas topi putih yang menyerang infrastruktur digital suatu organisasi saat penyerang jahat akan menguji pertahanan organisasi (juga dikenal sebagai "pengujian pena"). Tim merah dari calon keamanan siber adalah “Inti Kekuatan Oposisi Siber” yang secara etis mengeksploitasi sistem informasi dalam lingkungan yang terkendali dan tanpa niat jahat. Penilaian tim merah tidak mencari beberapa kerentanan tetapi kerentanan yang akan dicapai

tujuan mereka. Tujuannya seringkali sama dengan tes penetrasi.
Tim Merah menerapkan beberapa metode OSINT untuk mencapai tujuan mereka seperti Rekayasa Sosial yaitu mewawancarai karyawan untuk mengungkap informasi penting, serangan nirkabel untuk menguji keamanan Titik Akses, serangan eksternal untuk menguji perangkat perimeter, dan banyak lagi.

Penempatan tim merah sebagian besar cocok untuk organisasi dengan program keamanan yang matang. Organisasi yang sering melakukan pentest rutin, menambal sebagian besar kerentanan, dan umumnya memiliki hasil pentest positif. Tes tim merah yang intensif akan terjadi mengekspos faktor risiko yang berada pada teknologi, manusia, dan infrastruktur fisik.



Gambar -1: Tes Tim Merah

Selama keterlibatan tim merah, veteran keamanan yang sangat terlatih memerankan skenario serangan untuk mengungkap potensi kelemahan pada komponen fisik, perangkat keras, perangkat lunak, dan manusia dalam sistem informasi. Keterlibatan tim merah juga membuka peluang terjadinya serangan orang dalam yang membahayakan sistem dan jaringan atau memungkinkan pelanggaran data.

6. TIM MERAH VERSUS VAPT TRADISIONAL

Untuk menentukan risiko terhadap infrastruktur jaringan suatu organisasi, tanggung jawab utama operator Tim Merah adalah mengenali potensi ancaman atau kerentanan.
Berbagai macam alat sumber terbuka atau alat komersial dapat digunakan oleh Tim Merah untuk mengenali kerentanan dan mengeksploitasinya sesuai keinginan mereka. Pendekatan tim merah lebih mendalam daripada apa yang dilakukan oleh sebagian besar pelaku ancaman jahat ketika mereka berusaha menemukan satu kerentanan, sedangkan profesional keamanan perlu menemukan semua kemungkinan kerentanan pada sistem informasi tertentu untuk menilai dampak bisnis dari risiko tersebut. Anggota Tim Merah menguji semua kemungkinan serangan untuk memberikan penilaian keamanan lengkap terhadap sistem informasi. Kesadaran menyeluruh terhadap infrastruktur keamanan merupakan hasil penelitian Tim Merah secara mendetail

dari sistem informasi. Namun, Tim Merah tidak akan cukup dalam mengidentifikasi setiap risiko yang ada pada infrastruktur; organisasi harus selalu mempertahankan langkah-langkah keamanan yang ditargetkan untuk mengelola risiko dengan tepat dan memberikan perlindungan keamanan.

Pengujian pena digunakan untuk memantau, mengendalikan, dan mengidentifikasi kerentanan untuk mengamankannya serta menguji efisiensi prosedur manajemen kerentanan yang ditetapkan. Hal ini lebih lanjut membantu sekuler sebagai landasan dalam kebijakan keamanan informasi. Pengujian pena adalah pengujian lingkungan keamanan infrastruktur untuk menemukan dan menambal kerentanan dalam jangka waktu terbatas sehingga dapat dihilangkan

skenario positif palsu. Dibandingkan dengan Tim Merah, pengujian Pena adalah pengujian jaringan, perangkat keras, atau aplikasi yang paling ketat dan metodis. Selama pengujian Pena, penguji pena mencari kerentanan, menganalisisnya, dan mengeksploitasinya. Tes penetrasi didefinisikan dengan baik dan biasanya memakan waktu hingga satu hingga dua minggu untuk keseluruhan proses. Tim Merah mencakup taktik, teknik, dan prosedur (TTP) oleh musuh. Tim Merah sama seperti pengujian Pena dalam banyak hal tetapi lebih tepat sasaran. Tim Merah mengakses dan mengevaluasi berbagai bidang keamanan informasi secara komprehensif melalui jalur berlapis. Tujuannya adalah untuk mencoba meningkatkan respon perusahaan yaitu dengan menyajikan skenario dunia nyata. Setiap area keamanan informasi menentukan bagaimana target akan merespons atau bagaimana informasi tersebut diakses. Ini mengikuti konsep pertahanan secara mendalam; oleh karena itu, target harus diuji pada setiap lapisan.

Tujuan Tim Merah bukan untuk menemukan potensi kerentanan, melainkan untuk menguji kemampuan deteksi dan respons kerangka kerja serta status keamanannya. Penilaian kerentanan adalah proses menganalisis sistem yang berfokus pada menemukan kerentanan dan memprioritaskannya berdasarkan risiko. Eksploitasi atau dukungan terhadap suatu kerentanan tidak dilakukan saat penilaian kerentanan. Ketika penilaian kerentanan dibandingkan dengan keterlibatan Tim Merah tidak menjadi prioritas. Tim Merah tidak boleh menggunakan kerentanan apa pun. Tim Merah dapat mencapai dampak operasional yang dapat diterapkan oleh orang dalam untuk menguji umpan balik dari serangan orang dalam. Tim Merah jarang atau bahkan tidak pernah menyusun alat penilaian kerentanan umum karena alat tersebut keras dan mengeksekusi lebih banyak lalu lintas daripada yang dapat diterima oleh keterlibatan Tim Merah pada umumnya.

7. KERJA TIM MERAH

7.1 Emulasi Ancaman

Prosesnya meniru TTP dari ancaman tertentu. Tindakan ini dapat dilakukan untuk berbagai serangan seperti zero-day, script kiddie terhadap penyerang progresif, atau ancaman yang ditangani seperti botnet, ransom ware, DDOS, dll. Rintangan utama dalam emulasi ancaman adalah mensimulasikan ancaman ke tingkat di mana analis percaya bahwa itu nyata. Hal ini dapat dicapai mulai dari menggunakan malware nyata hingga mengembangkan muatan khusus, menggunakan alat untuk menghasilkan IOC (indikator kompromi).

7.2 Dampak Operasional

Tindakan atau efek yang dilakukan terhadap target yang dirancang untuk menunjukkan kelemahan fisik, informasi, atau operasional dalam infrastruktur keamanan diamati pada bagian Dampak Operasional. Dampak ini dapat bersifat umum seperti melakukan serangan penolakan layanan pada suatu layanan atau lebih spesifik seperti penggunaan Token SWIFT dengan jack tinggi untuk mengendalikan Transaksi SWIFT Internasional.

Dampak Operasional cukup dalam menunjukkan dampak yang masuk akal terhadap suatu target. Tingkat kedalaman dan dampaknya bisa sangat buruk jika manajemen aktif melakukan eksplorasi. Dampak ini biasanya dilakukan terhadap sistem produksi langsung untuk memiliki tingkat fidelitas tertinggi, namun dapat dijalankan pada lingkungan Pengujian Penerimaan Pengguna jika sistem tersebut merupakan sistem yang representatif.

8. TIM MERAH: ATURAN KETERLIBATAN

- Melaksanakan persyaratan keterlibatan sesuai petunjuk.
- Mematuhi semua undang-undang, peraturan, kebijakan, program, dan Aturan Keterlibatan.
- Menerapkan metodologi operasional Tim dan TTP.
- Mengidentifikasi dan mempunyai masukan terhadap lingkungan target kekurangan.
- Meneliti dan mengembangkan alat eksploitasi dan alat pengujian baru untuk fungsionalitas.
- Melakukan OSINT jika diperlukan untuk penugasan.

- Mengidentifikasi dan menilai tindakan yang mengungkapkan kerentanan sistem.
- Membantu Pimpinan Tim Merah dalam pengembangan laporan keterlibatan akhir.
- Melakukan dukungan Penilaian Fisik di bawah arahan Pimpinan Tim Merah.

9. KA CYBER LLP: VAPT VIRTUAL

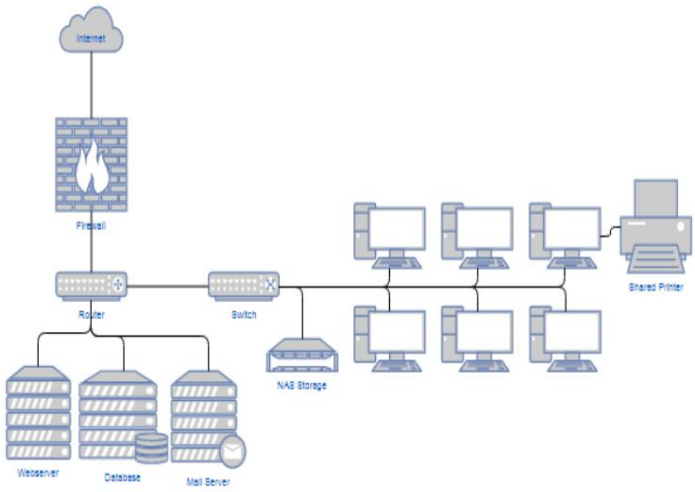
- Broken Walls Inc. terlibat untuk melakukan Uji Penetrasi pada sistem jaringan KA Cyber LLP dari Januari 2020 hingga April 2020. Tujuan Broken Walls Inc. adalah untuk menemukan kerentanan signifikan dalam infrastruktur jaringan KA Cyber LLP. Temuan ini akan digunakan dengan analisis risiko untuk membantu mengembangkan arsitektur keamanan untuk KA Cyber LLP.

- Temuan paling signifikan terkait dengan keseluruhan filosofi desain di balik model kepercayaan KA Cyber LLP, kurangnya skema Identifikasi dan Otentikasi (I&A) yang konsisten, penerapan dan kepatuhan terhadap kebijakan dan prosedur yang ada tidak konsisten dan tidak merata, kurangnya dukungan yang memadai pengendalian dan prosedur audit, dan sejumlah besar kerentanan yang mengakibatkan jaringan dan sistem rentan terhadap gangguan dari jaringan internal.

- Temuan pengujian penetrasi terperinci diurutkan berdasarkan tingkat keparahannya dan dibahas secara rinci dalam laporan eksekutif.

• Budaya dan filosofi perusahaan menentukan model kepercayaan. Model manajemen kepercayaan adalah dasar logis di mana arsitektur keamanan dibangun.
Arsitektur keamanan menyediakan kerangka umum untuk semua alat, kebijakan, dan prosedur keamanan lainnya. KA Cyber LLP memiliki model kepercayaan yang mengasumsikan pengguna internal jaringan dapat dipercaya. Model ini dirancang untuk memenuhi kebutuhan bisnis KA Cyber LLP di mana orang secara rutin berpindah lokasi di dalam gedung dan sumber daya perlu dialokasikan secara dinamis. Model ini dirancang untuk memiliki lingkungan bisnis yang lancar.

• Lingkungan yang berubah-ubah di KA Cyber LLP menciptakan situasi di mana tindakan pengendalian tidak dapat dengan mudah ditambahkan ke infrastruktur jaringan. Karena mekanisme kontrol akses yang tidak memadai, pelanggaran terhadap kebijakan dan prosedur saat ini yang tidak selalu dapat dicegah atau dideteksi di lingkungan sering terjadi. Selain itu, tidak ada mekanisme untuk memverifikasi dan tidak menyangkal identitas individu. Selain itu, beberapa ID pengguna dikelola secara lokal dan tidak ada di Direktori Aktif sehingga tidak konsisten di seluruh sistem. Kebijakan dan prosedur keamanan yang ada tidak dikelola secara merata, dan catatan audit serta informasi yang dikumpulkan dari berbagai sistem tidak ditinjau secara berkala. • Berikut adalah diagram virtual Cyber LLP.



Gambar -2: Contoh Lingkungan KA Cyber LLP

9. HASIL DAN PEMBAHASAN

Terlepas dari frekuensi pengujian kerentanan, tidak ada sistem kritis yang dianggap terlindungi dengan baik kecuali segmen jaringan dan host/server kritis dimonitor secara terus-menerus untuk melihat tanda-tanda upaya eksploitasi dan intrusi. Karena eksploitasi dan kerentanan baru dalam perangkat dan sistem operasi jaringan terdeteksi secara berkala, hal ini tidak dapat dibayangkan.

untuk memeriksa suatu jaringan secara menyeluruh, memberikan keamanan 100 persen karena kebal terhadap penetrasi baik dari dalam maupun dari luar. Selain itu, KA Cyber LLP telah memilih model kepercayaan di mana penerapan pengendalian internal yang lebih kuat akan lebih sulit dibandingkan dengan model kepercayaan yang lebih restrikt Oleh karena itu, metode terbaik untuk mendeteksi eksploitasi adalah dengan berbagai macam sistem deteksi intrusi yang berbasis jaringan dan dapat melakukan pembuatan profil pengguna. Tanpa pembagian identifikasi dan otentikasi pengguna, menganggap penyalahgunaan dilakukan oleh individu tertentu menjadi tidak dapat diandalkan. Tanpa pengendalian audit yang tepat untuk memastikan kepatuhan terhadap kebijakan, kebijakan dan prosedur itu sendiri menjadi tidak dapat dipertahankan.

Solusi Keamanan Tembok Rusak percaya bahwa tindakan perbaikan dan usulan dalam laporan ini akan meningkatkan kemampuan Layanan KA Cyber LLP untuk menghindari pelanggaran keamanan pengetahuan. Namun, Solusi Keamanan Tembok Rusak sangat menyarankan Deteksi dan Identifikasi Intrusi

dan Kemampuan Otentikasi ditambahkan ke jaringan untuk mendeteksi penyalahgunaan dan intrusi serta menyediakan data yang diperlukan untuk mendukung penyelidikan forensik. Hal ini juga didukung bahwa pengendalian audit untuk dinding yang rusak seperti pengujian kepatuhan, tinjauan log independen, atau audit konfigurasi diterapkan, dengan hasil dari pengendalian yang digabungkan tersebut dengan kesimpulan dari kemampuan deteksi intrusi. Tinjauan kebijakan dan prosedur, dikombinasikan dengan analisis risiko, bahkan akan sangat bermanfaat pada saat ini untuk menyederhanakan dan menegaskan kembali kebijakan-kebijakan yang penting bagi berfungsinya perusahaan.

10. KESIMPULAN

KA Cyber LLP kemudian mengalami kegagalan kontrol keamanan, yang mengakibatkan aset sampel perusahaan dikompromikan sepenuhnya. Kegagalan yang tampak kecil ini dapat berdampak buruk pada operasi bisnis jika dieksploitasi secara liar. Kebijakan penggunaan ulang kata sandi saat ini, model kepercayaan perusahaan, dan kurangnya mekanisme kontrol akses adalah penyebabnya

penyebab utama kegagalan untuk memitigasi dampak kerentanan yang ditemukan selama pengujian.

Serangan yang ditargetkan terhadap KA Cyber LLP dapat mengakibatkan kompromi total terhadap aset organisasi sehingga perusahaan tidak berdaya sama sekali. Berbagai permasalahan, yang biasanya dianggap kecil, dimanfaatkan secara bersamaan, sehingga mengakibatkan aset sampel KA Cyber LLP dikompromikan. Penting untuk dicatat bahwa runtuhnya infrastruktur keamanan KA Cyber LLP ini sebagian besar disebabkan oleh kurangnya kontrol akses pada batas jaringan dan tingkat host.

PENGAKUAN

Saya sangat berhutang budi kepada Universitas Raksha Shakti dan Sequretek IT Pvt. Ltd. atas bimbingan dan pengawasan terus-menerus serta untuk memberikan informasi yang diperlukan mengenai penelitian ini dan juga atas dukungan mereka dalam menyelesaikan upaya ini.

Saya ingin mengucapkan terima kasih yang sebesar-besarnya dan terima kasih kepada pembimbing internal dan eksternal saya Prof. Priyanka Sharma yang telah memberikan ilmu dan keahliannya dalam penelitian ini. Saya mengucapkan terima kasih yang sebesar-besarnya kepada Dekan Sekolah Teknologi Informasi dan Keamanan Siber Prof. Chandresh Parekh yang mengizinkan saya mengerjakan makalah penelitian ini dan dukungan mereka yang tiada henti dan luar biasa.

REFERENSI

[1]. Bradley J.Wood, Ruth A.Duggan, “Tim Merah Konsep Jaminan Informasi Tingkat Lanjut”, Pembelajaran,http://cs.uccs.edu/~cchow/pub/master/sjelinek/doc/research/red, [Diakses: 17 April 2020].

[2]. “Pendahuluan Ikhtisar Tim , Penilaian & Metodologi”, Merah, https:// [online].tersedia: resources.infosecinstitute.com/red-teaming-viewer-assessment-methodology/#gref , [Diakses: 17 April 2020].

[3]. “Perbedaan antara Penilaian Kerentanan dan Pengujian Penetrasi”[online].tersedia: https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/ , [Diakses: 20 April 2020].

[4]. Christopher Peake, “Red Teaming: The art of Ethical Hacking”, Metodologi Tim Merah, Jurnal SANS Institute, 2003, hal. 9-14

[5]. “Pengujian Penetrasi Tim Merah”[online].tersedia: https://www.coresecurity.com/what-red-team-security , [Diakses: 20 April 2020].

[6]. “Uji Penetrasi Penilaian Tim Merah: Perdebatan Lama Ninja Bajak Laut Berlanjut”, [online].tersedia: https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the -debat-usia-tua-bajak laut- vs-ninja-lanjutan/, [Diakses: 20 April 2020]

[7]. “Panduan Operasi Tim Merah”, Apa saja aspek dari tim Merah?, https://www.hackingarticles.in/guide-to-red-team-operations/ , [Diakses: 20 April 2020].

[8]. “Panduan Tim Merah”, Edisi Kedua, Keberhasilan Tim Merah, Peran Pengguna Akhir, Jurnal Komandan Pasukan Gabungan dan Kepala Staf, Januari 2013, hal. 2:1 - 3:11.

[9]. MegaCorp One, “Laporan Uji Penetrasi”, Eskalasi ke Administrator Lokal, Jurnal Layanan Keamanan Ofensif, Agustus 2013, hal. 6-12.

BIOGRAFI

Khushboo Amin, Magister Teknologi, Sekolah Teknologi Informasi dan Keamanan Siber, Universitas Raksha Shakti, Lavad, Gandhinagar, Gujarat, India.
Surel: khushbooamin@outlook.com

Priyanka Sharma, Dekan, Sekolah Penelitian & Pengembangan Teknologi Informasi & Keamanan Siber, Universitas Raksha Shakti, Lavad, Gandhinagar, Gujarat, India.
Email: ps.it@rsu.ac.in