PERBANDINGAN KEEFEKTIFAN ANTIVIRUS KASPERSKY DAN WINDOWS DEFENDER TERHADAP SERANGAN ADVANCED PERSISTENT THREAT

SKRIPSI

WALID BADEGES

2007422009

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

PERBANDINGAN KEEFEKTIFAN ANTIVIRUS KASPERSKY DAN WINDOWS DEFENDER TERHADAP SERANGAN ADVANCED PERSISTENT THREAT

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

WALID BADEGES

2007422009

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	:	Walid Badeges
NIM	:	2007422009
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	:	Perbandingan Keefektifan Antivirus Kaspersky dan *Windows Defender* Terhadap Serangan *Advanced Persistent Threat*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 20 Juli 2024

Yang membuat pernyataan

Walid Badeges

NIM. 2007422009

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Walid Badeges

NIM : 2007422009

Program Studi : Teknik Multimedia Jaringan

Judul Skripsi : PERBANDINGAN KEEFEKTIFAN ANTIVIRUS KASPERSKY DAN WINDOWS DEFENDER TERHADAP SERANGAN ADVANCED PERSISTENT THREAT

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin

Tanggal 30, Bulan Juli, Tahun 2024. dan dinyatakan **LULUS.**

Disahkan oleh		Tanda Tangan
Pembimbing I	: Defiana Arnaldy, S.Tp., M.Si.	
Penguji I	: Dr. Indra Hermawan, M.Kom.	
Penguji II	: Ayu Rosyida Zain, S.ST, M.T.	( )
Penguji III	: Iik Muhamad Malik Matin, S.Kom., M.Kom.	( )

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Dr., Anita Hidayati, S.Kom., M.Kom.
NIP. 197802112009121003

PENGANTAR

Puji syukur kehadirat Allah SWT, atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "Perbandingan Keefektifan Antivirus *Kaspersky* dan *Windows Defender* Terhadap Serangan *Advanced Persistent Threat*". Skripsi ini diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Terapan di Politeknik Negeri Jakarta.

Penulis menyadari bahwa dalam menyelesaikan skripsi ini, banyak pihak yang telah membantu dan memberikan dukungan. Oleh karena itu, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Defiana Arnaldy, S.TP., M.Si., atas bimbingan, arahan, dan masukan yang sangat berharga selama proses penyelesaian skripsi ini.
2. Ketua Jurusan, Dosen, dan Staf Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta, atas ilmu dan pengetahuan yang telah diberikan selama perkuliahan.
3. Orang tua dan keluarga, atas doa, dukungan moral, dan motivasi yang tiada henti-hentinya selama penulis menempuh pendidikan.
4. Teman-teman seperjuangan, atas semangat, motivasi, dan bantuannya selama perkuliahan dan penyelesaian skripsi.
5. Semua pihak yang telah membantu dan mendukung penulis dalam menyelesaikan skripsi ini, baik secara langsung maupun tidak langsung.

Penulis berharap skripsi ini dapat bermanfaat bagi para pembaca, khususnya dalam memahami simulasi serangan APT dan penerapan *Red Team C2* dalam upaya penetrasi testing. Penulis juga menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun untuk menyempurnakan skripsi ini di masa yang akan datang

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama	:	Walid Badeges
NIM	:	2007422009
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

PERBANDINGAN KEEFEKTIFAN ANTIVIRUS KASPERSKY DAN *WINDOWS DEFENDER* TERHADAP SERANGAN *ADVANCED PERSISTENT THREAT*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif in Politeknik Negeri Jakarta Berhak menyimpan, mengalihkamediakan/formatkan, mengelola dalam bentuk pangakalan data(database), merawat, dan mempublikasikan skripsinya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 20 Juli 2024

Yang membuat pernyataan

Walid Badeges

NIM. 2007422009

Perbandingan Keefektifan Antivirus *Kaspersky* dan *Windows Defender* Terhadap Serangan *Advanced Persistent Threat*

Abstrak

Penelitian ini mengidentifikasi masalah utama, yaitu kurangnya efektivitas metode konvensional dalam mengidentifikasi dan merespons ancaman Advanced Persistent Threat (APT) yang semakin canggih, serta meningkatnya frekuensi dan kompleksitas serangan siber yang menargetkan sistem informasi organisasi, menyebabkan kerugian besar dan kebocoran data. Solusi keamanan yang ada, seperti antivirus bawaan, sering kali tidak cukup efektif dalam mendeteksi dan mencegah serangan tersebut karena sifat serangan yang tersembunyi dan persisten, seperti yang ditunjukkan oleh penelitian sebelumnya yang hanya menggunakan Windows Defender sebagai solusi antivirus. Untuk mengatasi masalah ini, penelitian ini menggunakan teknologi Caldera C2 dan Cobalt Strike untuk melaksanakan simulasi serangan APT dengan tujuan mengidentifikasi dan mengevaluasi kerentanan dalam jaringan dan sistem yang dikelola. Penelitian ini juga menguji efektivitas dua produk antivirus, yaitu Kaspersky dan Windows Defender, dalam mendeteksi dan merespons serangan APT. Hasil pengujian menunjukkan bahwa Kaspersky berhasil mendeteksi serangan yang dilakukan dengan Caldera dan Cobalt Strike, sementara Windows Defender hanya mampu mendeteksi serangan dari Cobalt Strike. Pendekatan yang lebih komprehensif, termasuk penggunaan Red Team C2 dalam simulasi serangan APT dan pemilihan antivirus yang lebih tepat berdasarkan hasil pengujian, dapat meningkatkan perlindungan terhadap ancaman APT. Penelitian ini memberikan wawasan berharga tentang kerentanan sistem dan memberikan rekomendasi praktis tentang pemilihan solusi antivirus yang lebih efektif.

Kata kunci: Advanced Persistent Threat, Antivirus Kaspersky, Antivirus Windows Defender, Command and Control, Red Team.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, hampir setiap aspek kehidupan telah diwarnai oleh kemajuan teknologi, khususnya dengan penetrasi luas internet ke dalam masyarakat. Internet tidak hanya menjadi alat komunikasi, tetapi juga menjadi fondasi bagi berbagai aspek kehidupan sehari-hari seperti perbankan online, layanan kesehatan digital, interaksi sosial, dan pasar global. Namun, bersamaan dengan manfaatnya, pesatnya pertumbuhan internet juga membawa dampak negatif yang signifikan. Salah satu dampak yang paling mencolok adalah peningkatan tajam dalam kejahatan siber. (Ghelani, 2022)

Sebagai respons terhadap ancaman ini, praktik keamanan siber semakin berkembang. Salah satu pendekatan yang populer adalah penggunaan Red Team, sebuah tim yang disiapkan secara khusus untuk mensimulasikan serangan siber dari perspektif penyerang. Dengan menggunakan teknik dan alat yang sama seperti penyerang sungguhan, Red Team bertujuan untuk mengidentifikasi kelemahan dalam pertahanan siber suatu organisasi dan meningkatkan kesiapannya dalam menghadapi serangan. (Schlette, Böhm, Caselli, & Pernul, 2020).

Dalam konteks Indonesia, negara ini juga telah menjadi sasaran serangan siber yang serius. Kasus-kasus seperti serangan terhadap lembaga pemerintah, perusahaan swasta, dan infrastruktur kritis menyoroti urgensi perlunya peningkatan keamanan siber di tingkat nasional. Melalui pemahaman mendalam tentang serangan APT dan penerapan praktik-praktik Red Team serta penggunaan C2 dalam simulasi, dapat ditemukan langkah-langkah proaktif untuk melindungi sistem informasi dan infrastruktur kritikal di Indonesia dari ancaman yang semakin berkembang di ranah siber. (Iswardhana, 2021).

APT (*Advanced Persistent Threat*) dilakukan oleh para penyerang yang sangat berpengalaman dan memiliki sumber daya finansial yang besar, dengan tujuan untuk

mencuri informasi rahasia dari organisasi swasta. Salah satu tujuan utama dari APT adalah untuk mentransfer informasi yang disaring ke host eksternal, yang sering kali melibatkan pencurian dan eksfiltrasi data. Contoh konkret dari serangan APT termasuk pencurian 9 GB data kata sandi terenkripsi dari Adobe pada tahun 2013, serta pencurian 40 GB database Ashley Madison pada tahun 2015. (Abdullayeva, F. J, 2021).

Sebuah studi yang dilakukan oleh SophosLab pada tahun 2013 menunjukkan bahwa Indonesia memiliki tingkat paparan ancaman (Threat Exposure Rate) tertinggi di dunia. Tingkat paparan ancaman ini diukur berdasarkan persentase komputer yang terkena serangan malware dalam periode 3 bulan. Hasil penelitian tersebut mengungkapkan bahwa Indonesia menjadi target utama serangan siber. (Kurnia, 2023).

10 Riskiest Countries

	TER		TER
1. Indonesia	**23.54%**	6. India	**15.88%**
2. China	**21.26%**	7. Mexico	**15.66%**
3. Thailand	**20.78%**	8. UAE	**13.67%**
4. Philippines	**19.81%**	9. Taiwan	**12.66%**
5. Malaysia	**17.44%**	10. Hong Kong	**11.47%**

Gambar 1. 1 Riskiest Countries by SophosLab Report 2013 (SophosLab, 2013)

Sumber: (*Security Threat Report - SophosLab*, t.t.)

Praktik *Red Team* pada perangkat lunak antivirus juga memainkan peran krusial dalam pertahanan siber sehari-hari. Antivirus seperti Kaspersky dan Windows Defender menjadi pilihan umum dalam melindungi sistem terhadap berbagai jenis ancaman, termasuk APT. Penelitian yang membandingkan keefektifan antivirus ini terhadap serangan APT menjadi relevan dalam konteks perlindungan data sensitif dan infrastruktur kritis di Indonesia. (Barik, 2020)

Dengan demikian, fokus utama skripsi ini adalah untuk membandingkan efektivitas Antivirus Kaspersky dan Windows Defender dalam melindungi sistem terhadap

serangan Advanced Persistent Threat, dengan harapan hasilnya dapat memberikan wawasan yang berharga dalam meningkatkan strategi keamanan siber di Indonesia.

1.2 Rumusan Masalah

Berdasarkan hal-hal yang telah disampaikan pada latar belakang di atas, berikut rumusan masalahnya:

a. Bagaimana keefektifan *Kaspersky* dan *Windows Defender* dalam mendeteksi dan mencegah serangan *Advanced Persistent Threat* (APT)?.
b. Apa perbedaan tingkat efektif antara *Kaspersky* dan *Windows Defender* dalam menghadapi serangan *Advanced Persistent Threat* (APT)?
c. Faktor-faktor apa saja yang mempengaruhi perbedaan keefektifan antara *Kaspersky* dan *Windows Defender* dalam menangani serangan *Advanced Persistent Threat* (APT)?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang disusun agar ruang lingkup penelitian lebih terfokus, adalah:

a. Jenis Antivirus: Penelitian ini hanya akan membandingkan dua antivirus, yaitu *Kaspersky* dan *Windows Defender*.
b. Jenis Ancaman: Fokus penelitian ini hanya pada *serangan Advanced Persistent Threat* (APT), tidak termasuk jenis ancaman siber lainnya.
c. Lingkup Pengujian: Pengujian dilakukan pada lingkungan laboratorium dengan kondisi yang dikontrol, tidak termasuk kondisi dunia nyata yang mungkin lebih kompleks.
d. Metode Pengujian: Pengujian keefektifan dilakukan melalui simulasi serangan APT, menggunakan metode dan alat yang ditentukan sebelumnya.
e. Durasi Pengujian: Batasan waktu pengujian akan dibatasi dalam periode tertentu.
f. Versi Antivirus: Penelitian ini menggunakan versi terbaru dari *Kaspersky* Versi 21.18.5.438 dan *Windows Defender* pada saat penelitian dilakukan.

g. Parameter Keefektifan: Keefektifan diukur berdasarkan deteksi, pencegahan, dan respon terhadap serangan APT, tidak termasuk aspek lain seperti performa sistem atau pengalaman pengguna.
h. Sistem Operasi: Pengujian dilakukan pada sistem operasi Windows 10, tidak termasuk versi lain dari Windows atau sistem operasi lainnya.
i. Sumber Data: Data yang digunakan dalam penelitian ini berasal dari hasil pengujian langsung dan tidak mencakup data dari sumber eksternal atau pihak ketiga.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

a. Menganalisis Efektivitas Penggunaan Caldera dan Cobalt Strike dalam Simulasi APT: Mengevaluasi sejauh mana alat Red Team C2 seperti Caldera dan Cobalt Strike dapat mensimulasikan serangan APT secara realistis dan kompleks untuk mengidentifikasi kerentanan dalam sistem keamanan.
b. Mengidentifikasi Faktor-faktor yang Mempengaruhi Keberhasilan Simulasi APT: Menilai faktor-faktor yang memengaruhi keberhasilan atau kegagalan simulasi serangan APT yang dilakukan menggunakan Caldera dan Cobalt Strike dalam pengujian terhadap sistem keamanan.
c. Membandingkan Tingkat Keefektifan Kaspersky dan Windows Defender dalam Menghadapi Serangan APT: Mengukur dan membandingkan kemampuan deteksi dan respons Kaspersky dan Windows Defender terhadap serangan APT yang disimulasikan menggunakan Caldera dan Cobalt Strike.

1.4.2 Manfaat

a. Peningkatan Keamanan Siber: Penelitian ini membantu organisasi memahami keefektifan dua solusi antivirus populer dalam menghadapi serangan APT, sehingga dapat meningkatkan langkah-langkah keamanan siber mereka.
b. Pemilihan Antivirus yang Tepat: Dengan mengetahui kelebihan dan kekurangan Kaspersky dan Windows Defender dalam mendeteksi dan

menangkal serangan APT, organisasi dapat membuat keputusan yang lebih tepat dalam memilih antivirus yang sesuai dengan kebutuhan mereka.

c. Pengembangan Strategi Pertahanan: Hasil penelitian ini dapat digunakan sebagai dasar untuk mengembangkan strategi pertahanan yang lebih kuat dan efektif dalam menghadapi serangan siber yang semakin kompleks.

d. Kesadaran dan Edukasi: Penelitian ini dapat meningkatkan kesadaran tentang ancaman APT dan pentingnya penggunaan alat keamanan yang tepat, sehingga mendorong edukasi dan peningkatan kapasitas dalam bidang keamanan siber.

e. Kontribusi terhadap Penelitian Keamanan Siber: Penelitian ini menambah literatur ilmiah di bidang keamanan siber, khususnya terkait dengan efektivitas antivirus dalam melawan serangan APT, sehingga dapat menjadi referensi bagi penelitian-penelitian selanjutnya.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam membuat laporan penelitian ini:

1. BAB I PENDAHULUAN

   Bab ini merupakan langkah awal dalam penulisan sistematika penelitian. Bab pendahuluan berisikan latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian serta sistematika penulisan.

2. BAB 2 TINJAUAN PUSTAKA

   Bab tinjauan pustaka merupakan bab kedua dalam sistematika penulisan pada penelitian ini. Bab ini berisikan tentang penguraian landasan teori yang digunakan dalam penelitian dan berisikan penguraian penelitian-penelitian terkait.

3. BAB III METODE PENLITIAN

   Bab metode penelitian merupakan bab ketiga dalam sistematika penulisan pada penelitian ini. Bab metode penelitian berisikan uraian tahapan penelitian, skenario analisis dan objek penelitian.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab hasil dan pembahasan merupakan bab keempat dalam sistematika penulisan pada penelitian ini. Bab hasil dan pembasahan berisikan uraian mengenai perancangan dan realisasi sistem juga proses analisis.

5. BAB V PENUTUP

   Bab penutup merupakan bab terakhir dalam sistematika penulisan pada penelitian ini. Bab ini berisikan tentang kesimpulan dan saran berdasarkan hasil analisis

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini telah berhasil mengimplementasikan dan menguji penggunaan Red Team Command and Control (C2) menggunakan alat Caldera dan Cobalt Strike dalam simulasi serangan Advanced Persistent Threat (APT). Pengujian ini dilakukan untuk mengidentifikasi dan mengevaluasi kerentanan dalam sistem keamanan informasi, khususnya dalam mendeteksi dan merespons serangan APT. Hasil pengujian menunjukkan bahwa Windows Defender tidak mampu mendeteksi serangan dari Caldera C2, sementara Kaspersky berhasil mendeteksi dan memblokir serangan tersebut. Namun, Cobalt Strike terbukti tidak efektif dalam simulasi serangan APT ini.

Hal ini menegaskan bahwa penggunaan alat Red Team C2 seperti Caldera sangat efektif dalam mensimulasikan serangan dan mengidentifikasi kelemahan dalam sistem keamanan, sementara Cobalt Strike mungkin memerlukan konfigurasi atau penyesuaian lebih lanjut untuk mencapai tingkat efektivitas yang sama. Penelitian ini juga menunjukkan pentingnya pemilihan solusi antivirus yang tepat untuk meningkatkan perlindungan terhadap ancaman siber yang semakin kompleks dan berkembang.

Penelitian ini menunjukkan perbedaan yang signifikan dalam tingkat keefektifan antara Kaspersky dan Windows Defender dalam mendeteksi dan mencegah serangan APT. Kaspersky terbukti lebih efektif dalam mendeteksi dan memblokir serangan yang disimulasikan menggunakan Caldera C2, sementara Windows Defender tidak mampu mendeteksi serangan tersebut. Perbedaan ini mengindikasikan bahwa Kaspersky memiliki kemampuan yang lebih canggih dalam mengenali pola-pola serangan APT, serta menerapkan mekanisme pencegahan yang lebih kuat dibandingkan dengan Windows Defender.

Ada beberapa faktor yang mempengaruhi perbedaan keefektifan antara kedua solusi antivirus ini. Pertama, Kaspersky dilengkapi dengan teknologi deteksi berbasis heuristic dan machine learning yang lebih maju, yang memungkinkan deteksi proaktif terhadap serangan baru dan belum dikenal. Kedua, Kaspersky memiliki database ancaman yang lebih luas dan sering diperbarui, yang membantu dalam mendeteksi varian-varian baru dari serangan APT. Ketiga, arsitektur keamanan Kaspersky dirancang untuk merespons ancaman secara real-time dengan lebih efektif, termasuk dalam mengidentifikasi dan memblokir aktivitas mencurigakan yang mungkin tidak terdeteksi oleh antivirus yang kurang canggih seperti Windows Defender.

5.2 Saran

Berdasarkan hasil penelitian ini, terdapat beberapa saran yang dapat diberikan untuk peningkatan keamanan sistem informasi:

1. **Pemilihan Solusi Antivirus:**
   Dalam pemilihan solusi antivirus, organisasi harus mempertimbangkan efektivitas antivirus dalam mendeteksi serangan APT. Penelitian ini menunjukkan bahwa Kaspersky lebih efektif dibandingkan Windows Defender dalam mendeteksi serangan dari Caldera C2 dan Cobalt Strike. Oleh karena itu, penting bagi organisasi untuk memilih solusi keamanan yang memiliki kemampuan deteksi yang unggul terhadap ancaman-ancaman terbaru.

2. **Pelatihan dan Kesadaran:**
   Meningkatkan pelatihan dan kesadaran bagi tim keamanan siber tentang teknik dan alat yang digunakan dalam serangan APT, serta bagaimana cara mendeteksinya. Dengan memahami bagaimana serangan ini bekerja, tim keamanan dapat merespons dengan lebih cepat dan efektif.

3. **Peningkatan Sistem Keamanan:**

   Organisasi harus secara rutin mengevaluasi dan meningkatkan sistem keamanan mereka, termasuk memperbarui perangkat lunak keamanan dan menerapkan praktik keamanan terbaik untuk melindungi terhadap ancaman siber yang terus berkembang. Evaluasi berkala terhadap efektivitas alat keamanan yang digunakan sangat penting untuk memastikan perlindungan yang optimal.

4. **Kolaborasi dan Berbagi Informasi:**

   Mendorong kolaborasi dan berbagi informasi antara organisasi untuk meningkatkan pemahaman kolektif tentang ancaman APT dan cara terbaik untuk mengatasinya. Berbagi informasi mengenai serangan yang terdeteksi dan cara penanggulangannya dapat membantu dalam memperkuat pertahanan secara keseluruhan

Dengan menerapkan saran-saran ini, diharapkan organisasi dapat meningkatkan kesiapsiagaan mereka dalam menghadapi ancaman siber dan melindungi aset informasi mereka secara lebih efektif.

DAFTAR PUSTAKA

Ghelani, D. (2022, September 22*). Cyber security, cyber threats, implications and future perspectives: A review*. https://doi.org/10.22541/au.166385207.73483369/v1

Schlette, D., Böhm, F., Caselli, M. *et al. Measuring and visualizing cyber threat intelligence quality*. *Int. J. Inf. Secur.* **20**, 21–38 (2021). https://doi.org/10.1007/s10207-020-00490-y

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cyber-security culture framework. *Sensors*, 21(9), 3267. https://doi.org/10.3390/s21093267

Abdullayeva, F. J. (2021). *Advanced Persistent Threat* attack detection method in cloud computing based on autoencoder and softmax regression algorithm. *Array*, 10, 100067. https://doi.org/10.1016/j.array.2021.100067

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials, 21, 1851-1877. https://doi.org/10.1109/COMST.2019.2891891.

Chatzigiannis, P., & Chalkias, K. (2022). Base64 Malleability in Practice. Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. https://doi.org/10.1145/3488932.3527284.

Kurniawan, M., Putra, I., Maheswara, I., Labamaking, R., Listartha, I., & Saskara, G. (2023). ANALISIS EFEKTIVITAS DAN EFISIENSI METODE ENCODING DAN DECODING ALGORITMA BASE64. Jurnal Informatika Dan Tekonologi Komputer (JITEK). https://doi.org/10.55606/jitek.v3i1.897.

Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., & Loukas, G. (2023). SoK: The MITRE ATT&CK Framework in Research and Practice. ArXiv, abs/2304.07411. https://doi.org/10.48550/arXiv.2304.07411.

Al-Sada, B., Sadighian, A., & Oligeri, G. (2023). MITRE ATT&CK: State of the Art and Way Forward. ArXiv, abs/2308.14016. https://doi.org/10.48550/arXiv.2308.14016.

Akuffo-Badoo, E. (2022). Understanding Advanced Persistent Threats. Advances in Multidisciplinary and scientific Research Journal Publication. https://doi.org/10.22624/aims/crp-bk3-p3.

Brandão, P., Mamede, H., & Correia, M. (2023). Advanced Persistent Threats Campaigns and Attribution. Journal of Computer Science. https://doi.org/10.3844/jcssp.2023.1015.1028.

Quintero-Bonilla, S., & Rey, Á. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. Applied Sciences. https://doi.org/10.3390/app10113874.

Smith, J., Theisen, C., & Barik, T., 2020. A Case Study of Software Security Red Teams at Microsoft. In: *2020 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. Dunedin, New Zealand: IEEE, pp. 1-10. doi:10.1109/VL/HCC50065.2020.9127203.

Schlette, D., Böhm, F., Caselli, M. et al., 2021. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, 20, pp. 21-38. https://doi.org/10.1007/s10207-020-00490-y.

Abdullayeva, F.J., 2021. Advanced Persistent Threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm. *Array*, 10, 100067. https://doi.org/10.1016/j.array.2021.100067.

Ghelani, Diptiben. "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review." Authorea, September 22, 2022. DOI: 10.22541/au.166385207.73483369/v1.

Alshamrani, A., Myneni, S., Chowdhary, A., and Huang, D., 2019. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*, 21(2), pp. 1851-1877. Available at: https://doi.org/10.1109/COMST.2019.2891891.

Phillips, D. and Milenkoski, A., 2019. Windows Defender Application Control: Initialization (Doctoral dissertation, ERNW Enno Rey Netzwerke GmbH).

DAFTAR RIWAYAT HIDUP

Walid Badeges

Lahir di Bogor pada 30 September 2002. Lulus dari SDN Pengadilan 3 tahun 2014, SMP PGRI 5 tahun 2017, SMA Bina Bangsa Sejahtera 2020. Pendidikan Profesi CEP-CCIT di Fakultas Teknik Universitas Indonesia (2020-2022) program studi Network Administrator Professional. Saat ini, sedang menyelesaikan studi D4 Teknik Informatika dan Komputer di Politeknik Negeri Jakarta (2020-2024) program studi Teknik Multimedia dan Jaringan, konsentrasi keamanan sistem informasi.