JUSIFO
JURNAL SISTEM INFORMASI

p-ISSN: 2460-092X, e-ISSN: 2623-1662
Vol. 9, No. 1, Juni 2023
Hal. 33 - 44

Analisis Keamanan Infrastruktur Jaringan Berdasarkan *Cyber Kill Chain Framework*

Utama Hasiolan Panggabean, Benfano Soewito*
bsoewito@binus.edu*
*Penulis korespondensi

Universitas Bina Nusantara - Indonesia

Diterima: 23 Mei 2023 | Direvisi: 05 Mei – 02 Jun 2023
Disetujui: 24 Jun 2023 | Dipublikasi: 30 Jun 2023
Program Studi Sistem Informasi, Fakultas Sains dan Teknologi,
Universitas Islam Negeri Raden Fatah Palembang, Indonesia

ABSTRACT

This study concentrates on examining the security of network infrastructure using the cyber kill chain framework approach. The research is conducted within a company operating in network security services. In its operations, it offers a Virtual Private Cloud (VPC) containing various crucial information such as applications, internal data, client data, and product demos. Despite the attractive features of cloud computing, there are significant threats as well. Handling attacks cannot be swiftly and efficiently executed, resulting in temporary operational unavailability until the attacks are resolved. This research delves into the security of the company's infrastructure by testing several points of vulnerability exploited by malicious parties. The cyber kill chain framework approach is employed to systematically assess the company's infrastructure. The study reveals that certain issues have been adequately detected; however, security gaps persist, as evidenced by the testing conducted and the inadequate response from the company's security systems.

Keywords: *Infrastructure Security Analysis, Security Gaps, Cyber Kill Chain Framework*

ABSTRAK

Penelitian ini berfokus pada analisis keamanan infrastruktur jaringan dengan menggunakan pendekatan cyber kill chain framework. Penelitian dilakukan pada perusahaan yang bergerak di bidang layanan keamanan jaringan. Dalam operasionalnya, perusahaan menawarkan Virtual Private Cloud (VPC) yang berisi berbagai informasi penting seperti aplikasi, data internal, data klien, dan demo produk. Meskipun cloud computing memiliki fitur menarik, terdapat ancaman serius juga. Penanganan serangan tidak dapat dilakukan dengan cepat dan efisien, sehingga menyebabkan ketersediaan operasional terganggu sementara waktu sampai serangan dapat diatasi. Penelitian ini membahas tentang keamanan infrastruktur perusahaan dengan menguji beberapa titik celah keamanan yang dieksploitasi oleh pihak yang tidak bertanggung jawab. Pendekatan kerangka kerja cyber kill chain digunakan untuk menilai infrastruktur perusahaan secara sistematis. Hasil penelitian menunjukkan bahwa beberapa masalah telah berhasil dideteksi dengan baik, namun celah keamanan masih ada, sebagaimana terlihat dari pengujian yang dilakukan dan kurangnya respon sistem keamanan perusahaan.

Kata Kunci: *Analisis Keamanan Infrastruktur, Celah Keamanan, Kerangka Kerja Cyber Kill Chain*

PENDAHULUAN

Saat ini, *cloud computing* telah menjadi alternatif *platform* komputasi yang penggunanya meningkat secara signifikan dalam beberapa tahun terakhir karena fiturnya. Dengan adanya *Cloud Computing*, memungkinkan pengguna baik organisasi maupun individu untuk mengakses sumber daya komputasi secara efisien, ekonomis, dan fleksibel, serta mengurangi kebutuhan akan investasi dalam infrastruktur fisik dan pemeliharaan. Selain itu, istilah *cloud computing* merujuk pada model komputasi yang berasal dari konsep komputasi grid, komputasi terdistribusi, komputasi paralel, teknologi virtualisasi, komputasi utilitas, dan teknologi komputer lainnya, cloud computing menawarkan berbagai keunggulan yang mencakup kemampuan untuk melakukan komputasi skala besar, penyimpanan data, virtualisasi, serta fleksibilitas tinggi, keandalan yang tinggi (Alouffi et al., 2021; Kumar et al., 2018; Liu, 2012; Tabrizchi & Kuchaki Rafsanjani, 2020). Suatu perusahaan yang bergerak untuk menyediakan infrastruktur keamanan jaringan komputer, tentunya dalam operasionalnya menawarkan *Virtual Private Cloud (VPC)* yang berisi banyak informasi penting seperti aplikasi, data internal, data klien, dan demo produk. Akan tetapi, meskipun *cloud computing* memiliki fitur menarik, juga terdapat ancaman serius (Bollinadi & Damera, 2017; Khalil et al., 2014; Zissis & Lekkas, 2012). Beberapa ancaman yang umum terjadi seperti: *brute force attacks*, *Denial of Service (DoS), ransomware*, peretasan akun, *phishing*, dan *malware* serta *virus* yang menyerang infrastruktur jaringan perusahaan (Carella et al., 2017; Ghafir et al., 2018; Gunduz & Das, 2020; Rehak et al., 2019; Walker-Roberts et al., 2018).

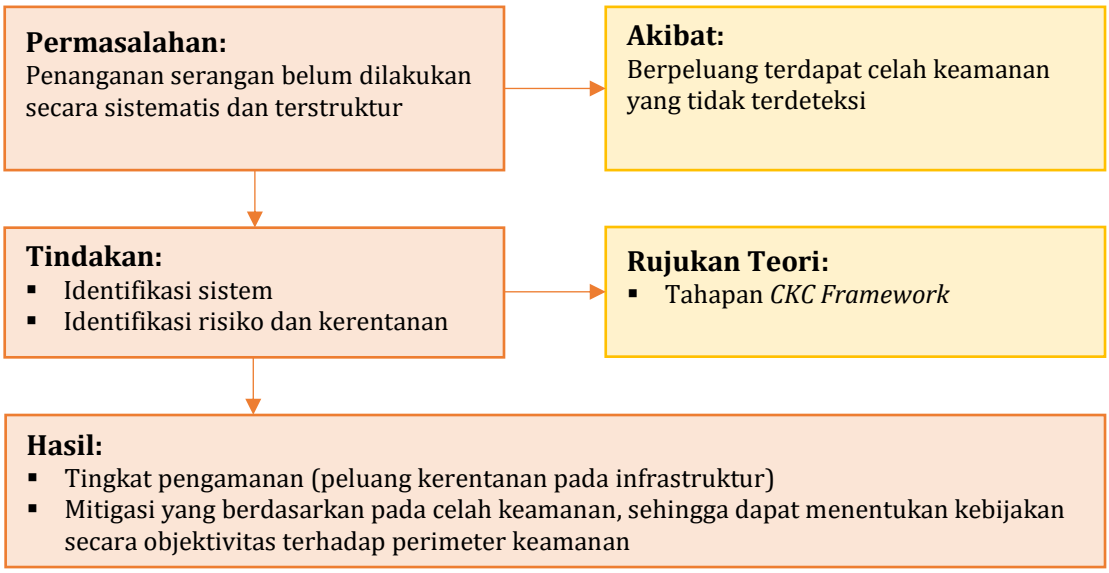
Penanganan serangan tidak dapat dilakukan dengan cepat dan efisien sehingga berdampak pada ketersediaan operasional untuk sementara waktu sampai serangan dapat diatasi. Secara umum, efek dari serangan-serangan tersebut adalah kehilangan akses ke infrastruktur dan aplikasi, kehilangan data, tidak tersedianya operasional perusahaan karena infrastruktur terganggu, dan juga hilangnya kepercayaan klien. Konsep keamanan yang terkait dengan kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* selalu dilibatkan dalam proses pengelolaan keamanan terkait dengan penggunaan jaringan *internet* (Abdul-Jabbar et al., 2020; Aminzade, 2018; Khidzir et al., 2018; Tchernykh et al., 2019). Penelitian ini membahas terkait keamanan infrastruktur perusahaan dengan melakukan pengujian terhadap beberapa titik dari celah keamanan yang dilakukan oleh pihak-pihak yang tidak bertanggungjawab.

Analisis keamanan yang dilakukan guna memberikan fakta-fakta terkini dari infrastruktur perusahaan, dalam hal ini perusahaan yang bergerak di bidang pelayanan keamanan jaringan. Penelitian ini berfokus pada analisis keamanan infrastruktur jaringan dengan menggunakan pendekatan *Cyber Kill Chain Framework (CKC Framework)*. Penggunaan *CKC Framework* telah diterapkan di beberapa bidang seperti perbankan (Kiwia et al., 2018), sistem *Internet of Things (IoT)* (Ahmed et al., 2021), dan sistem kontrol industri (Wang et al., 2021). Selain itu, pendekatan *CKC Framework* digunakan untuk mendeteksi serangan secara komprehensif suatu infrastuktur di berbagai perusahaan (Abdul-Jabbar et al., 2020; Capano, 2019; Garba et al., 2019; Lee et al., 2021).

METODOLOGI PENELITIAN

Kerangka Berpikir

Penelitian ini dijalankan dengan merujuk pada tahapan yang dilakukan secara sistematis. Kerangka berpikir dibuat secara teliti dengan mempertimbangkan beberapa teori. Secara lengkap dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Berpikir

Proses Deteksi Kerentanan

Matriks kontrol *Cyber Kill Chain* (Gambar 2), digunakan pada penelitian ini untuk mendeteksi kerentanan yang mungkin dapat terjadi. Matriks tersebut dapat memberikan pemahaman kepada organisasi untuk mengembangkan strategi pertahanan yang sesuai. Dengan memahami langkah-langkah yang biasa dilakukan oleh *attacker* dan menerapkan kontrol yang sesuai di setiap tahapan, organisasi dapat meningkatkan kemampuan mereka dalam mendeteksi *(detect)*, mencegah akses yang tidak sah *(deny)*, mengubah atau menghentikan aliran informasi data ke *attacker (disrupt)*, membatasi efektivitas atau efisiensi serangan *(degrade)*, mengganggu serangan dengan menggunakan penyimpangan atau informasi palsu *(deceive),* dan membatasi lingkup serangan pada segmen-segmen tertentu dari jaringan atau perusahaan *(contain)*.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaisance						
Weaponization						
Delivery						
Exploitation						
Installation						
Command & Control						
Actions on Objectives						

Gambar 2. Matriks Kontrol *Cyber Kill Chain*

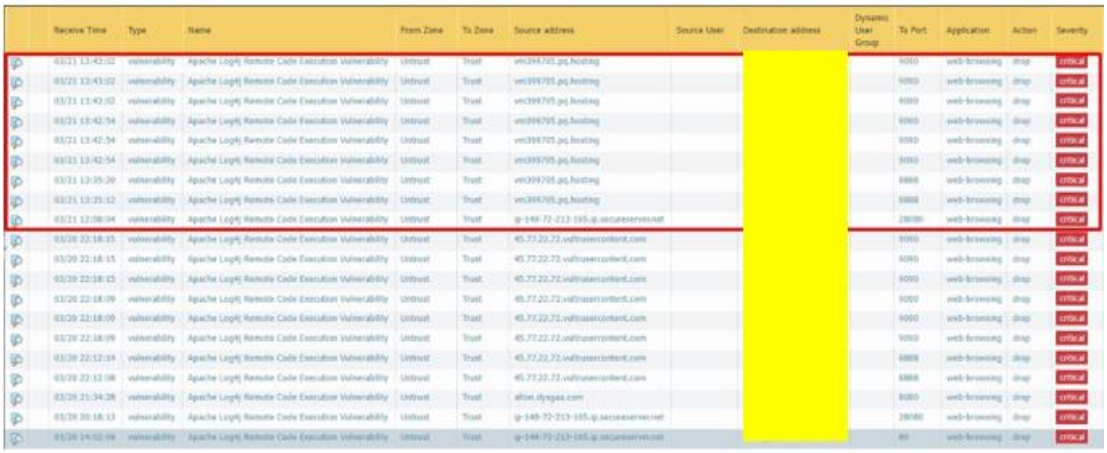
HASIL DAN PEMBAHASAN

Analisis Berdasarkan *CKC Framework*

CKC Framework digunakan untuk memahami, mendeteksi, dan menganalisis serangan *cyber* terhadap infrastuktur organisasi. Pada penelitian ini, dilakukan beberapa tahapan, seperti: *Reconnaissance* merujuk pada tindakan *attacker* dalam pengumpulan informasi, *Weaponization* merujuk pada tindakan *attacker* dalam memilih alat untuk mengekploitasi kerentanan, *Delivery* merujuk pada percobaan serangan awal dengan

mengirimkan alat ke target, *Exploitation* merujuk pada ekploitasi pada infrastruktur target, *Installation* merujuk pada pemasangan *malware* atau akses *backdoor* pada infrastruktur target, *Command and Control* merujuk pada tindakan *attacker* dengan melakukan komunikasi ke infrastuktur yang terinfeksi, dan *Actions on Objectives* merujuk pada tindakan akhir *attacker* seperti mencuri data dan menganggu infrastuktur target.

Pengujian pada tahap ***reconnaissance*** dilakukan untuk menemukan infrastruktur yang memiliki kerentanan *log4shell* yang merupakan kerentanan *zero-day* di java, keberhasilan serangan ini berdampak server dapat diambil alih oleh *attacker*. Dengan menggunakan *NMAP* dilakukan *recon* terhadap kelemahan *log4shell* menargetkan aplikasi perusahaan. Pada kegiatan pengujian tersebut dilakukan pengujian terhadap 10 IP Publik yang dimiliki oleh perusahaan, dengan melakukan *discovery open port* 443 dan 80. Selanjutnya, setelah ditemukannya *port* yang terbuka, maka dilanjutkan aktivitas pengujian dengan menjalankan *script NMAP* untuk mendeteksi apakah *port* yang terbuka tersebut apakah memiliki kelemahan *zero-day Log4shell* atau tidak. Hasil dari pengujian ini dapat dilihat pada Gambar 3.

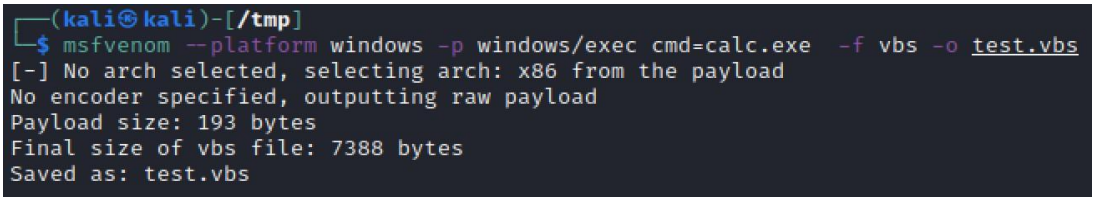


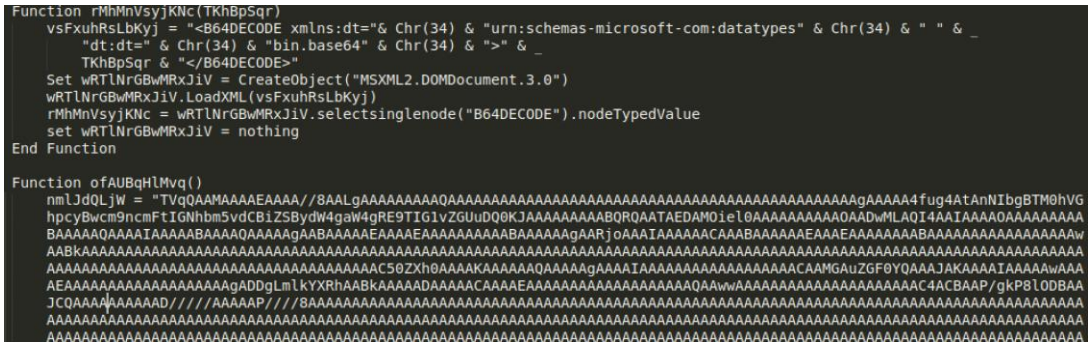
Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
☑	☑	✕	✕	✕	✕

Gambar 3. Pengujian Tahap *Reconnaissance*

Pada Gambar 3, diketahui bahwa sistem perusahaan dapat mendeteksi dan mencegah terhadap upaya *reconnaissance*. Hal tersebut dibuktikan dengan munculnya *alert* atau *event* pada *firewall* yang diterapkan oleh perusahaan, dimana *alert* tersebut memiliki status *DROP*, dengan kata lain *network packet* yang berasal dari kegiatan *reconnaissance* tersebut tidak diteruskan sampai ke target. *Network packet* tersebut di-*drop* secara otomatis oleh *firewall* karena terdeteksi sebagai *malicious packet*.

Pengujian pada tahap ***weaponization*** dilakukan percobaan dengan membuat *malicious vbscript* menggunakan *tools open source*. Pada percobaan tersebut menggunakan *msfvenom* untuk membuat file *vbs* sederhana yang berfungsi untuk memanggil fungsi kalkulator apabila file tersebut diakses atau dijalankan (Gambar 4).





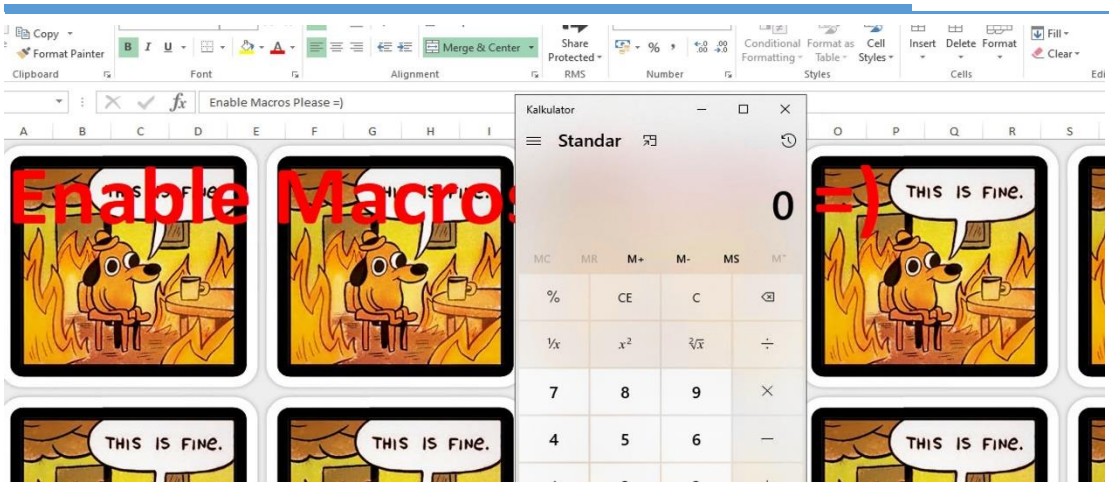
Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
✕	✕	✕	✕	✕	✕

Gambar 4. Pengujian Tahap *Weaponization*

Dari pengujian pada Gambar 4, diketahui bahwa infrastruktur perusahaan yang menggunakan sistem keamanan di dalamnya masih belum dapat mendeteksi ataupun mencegah percobaan yang dilakukan. Hal ini terlihat ketika *phase delivery* dijalankan, file *vbs* tersebut dapat sampai ke target.

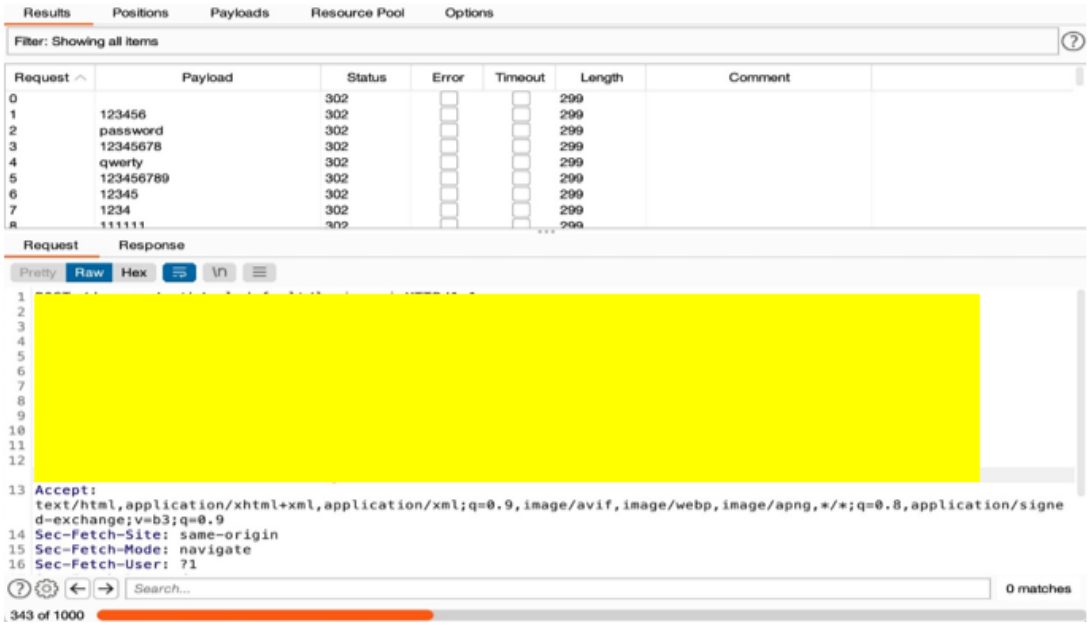
Pengujian pada tahap ***delivery*** dilakukan simulasi pengiriman email *phishing* yang berisi lampiran *malware* dengan baris subjek yang meminta pengguna untuk mengklik. Pada penelitian ini, pengguna melakukan eksekusi malware dalam bentuk dokumen atau program setelah *attacker* berhasil mengirimkan *malware* ke komputer pengguna (Gambar 5). Dari pengujian tersebut dapat diketahui bahwa teknologi yang digunakan oleh perusahaan masih belum dapat mendeteksi maupun mencegah aktivitas yang mencurigakan.

Pengujian pada tahap ***exploitation*** dilakukan percobaan serangan *brute force* yang menargetkan akses *Virtual Private Network (VPN)* dalam skenario ini *attacker* menebak *password* dari salah satu pengguna. Dari aktivitas yang dilakukan diketahui bahwa teknologi keamanan yang digunakan oleh perusahaan tidak dapat mengetahui ada aktivitas yang mencurigakan pada trafik *VPN*-nya. Hal ini terlihat pada Gambar 6 ketika dilakukan *burpsuite* sebagai alat melakukan serangan *brute force*, perusahaan masih belum dapat mecegah maupun mendeteksi aktivitas tersebut.



Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
✗	✗	✗	✗	✗	✗

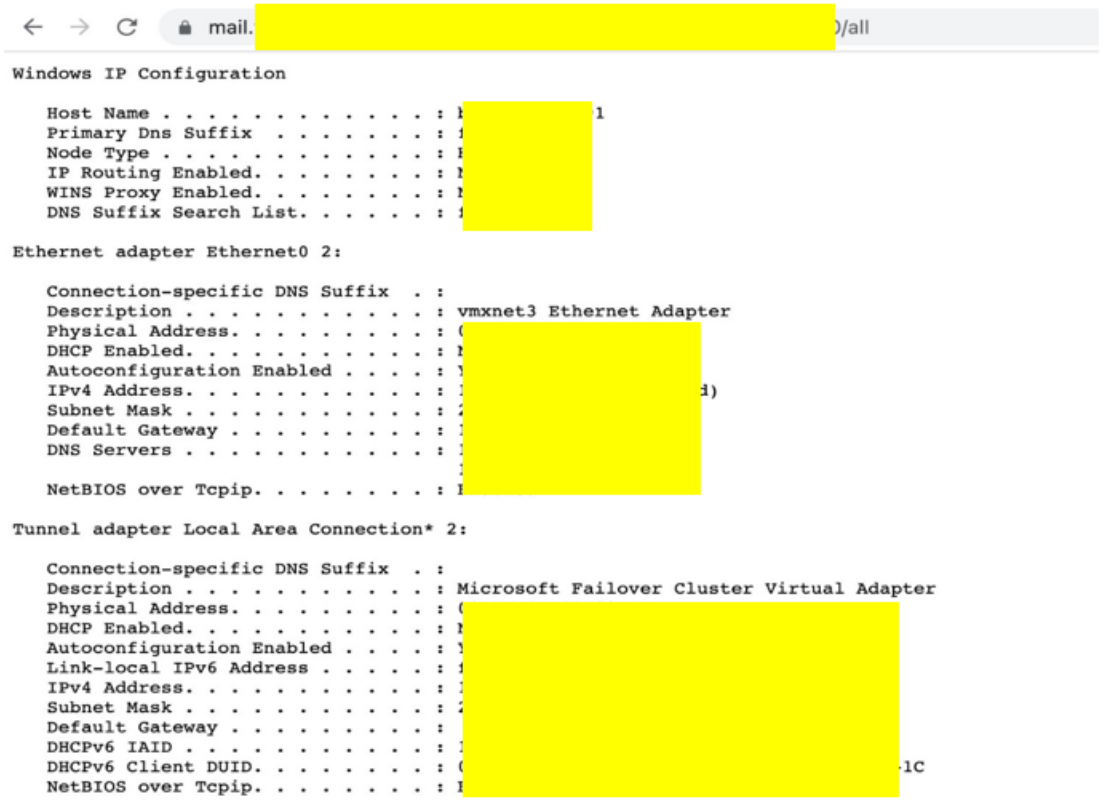
Gambar 5. Pengujian Tahap *Delivery*



Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
✗	✗	✗	✗	✗	✗

Gambar 6. Pengujian Tahap *Exploitation*

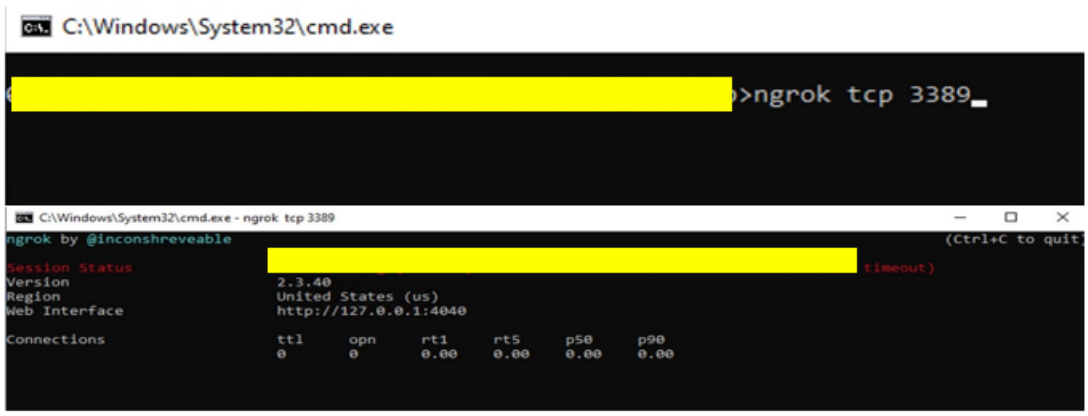
Pengujian pada tahap ***installation*** dilakukan simulasi dengan skenario bahwa *attacker* mencoba memasang *webshell backdoor* pada *web server* yang telah dikenali digunakan sebagai akses masuk kembali ke dalam sistem. Pengujian menunjukkan bahwa *attacker* telah berhasil masuk ke dalam *Microsoft Exchange Server* dan memasang *webshell* dan menjalankan perintah secara *remote* melalui *web browser*. Adapun perintah yang dicontohkan adalah *ipconfig* pada *webshell*. Hal ini dapat dilihat pada Gambar 7 yang menunjukkan aktivitas *webshell* tersebut berhasil dengan memberikan respon langsung pada tampilan *web browser*.

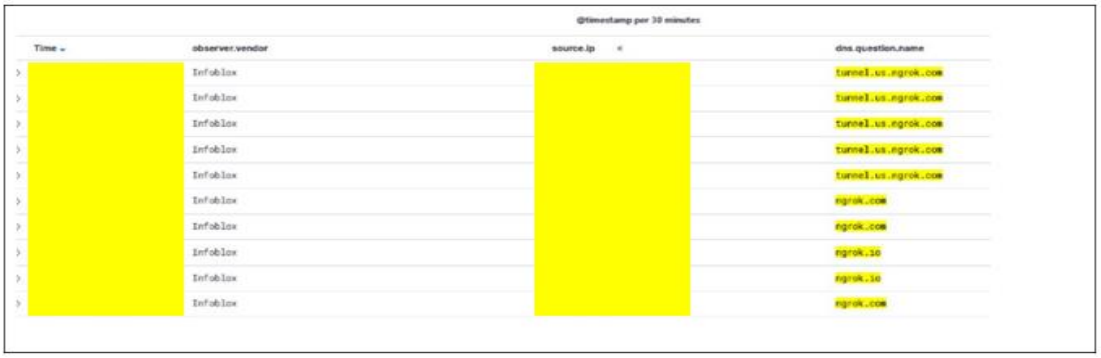


Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
✕	✕	✕	✕	✕	✕

Gambar 7. Pengujian Tahap *Installation*

Pengujian pada tahap ***command and control*** digunakan teknik *network tunnel* dari sistem target (korban) dalam protokol terpisah untuk menghindari deteksi atau proses filter jaringan dan/atau memungkinkan akses ke sistem yang tidak terjangkau. *Tunneling* melibatkan enkapsulasi protokol secara eksplisit di dalam protokol lain. Tindakan ini dapat menyembunyikan lalu lintas berbahaya dengan menggabungkan lalu lintas yang ada dan/atau menyediakan lapisan enkripsi luar (mirip dengan *VPN*). Seperti yang terlihat pada Gambar 8, digunakan *Ngrok*. *Ngrok* adalah alat reverse *proxy* yang dapat membuat *tunneling* ke *server* yang terletak di belakang *firewall* atau di mesin lokal yang tidak memiliki *IP* publik.



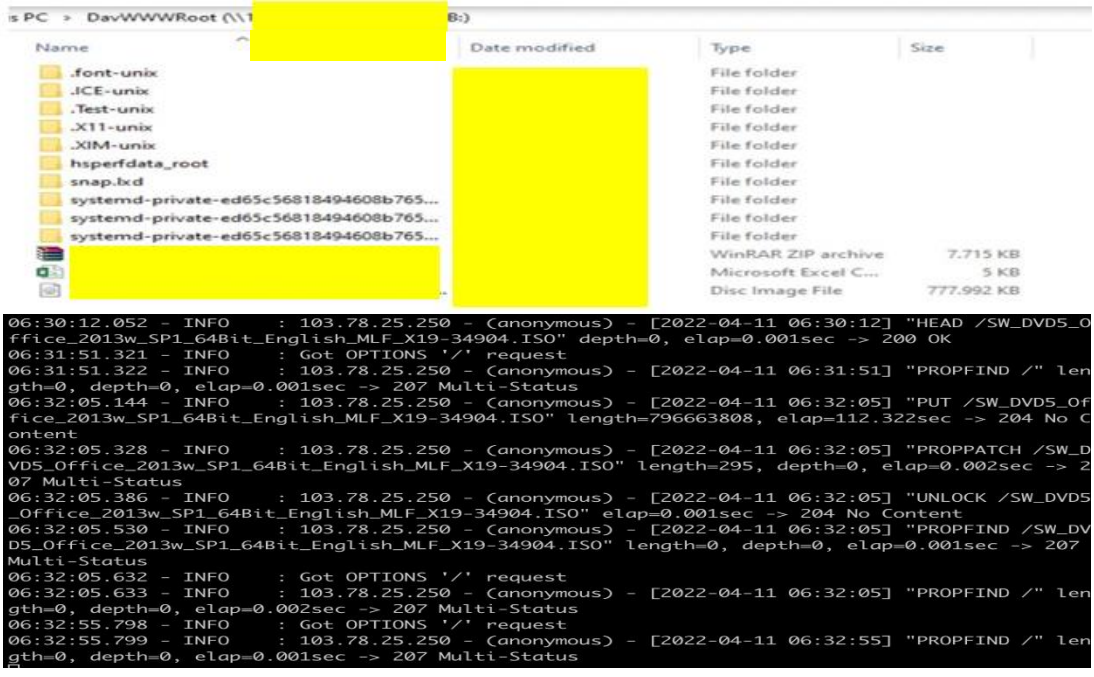


Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
☑	✗	✗	✗	✗	✗

Gambar 8. Pengujian Tahap *Command and Control*

Dari pengujian (Gambar 8), dilakukan upaya menjalankan *tunnel* dengan melakukan *listening* pada *port* 3389, namun hal tersebut dapat dideteksi oleh teknologi keamanan yang dimiliki oleh perusahaan, dalam hal ini teknologi yang dapat melakukan deteksi adalah *Proxy*, namun belum dapat dicegah. Hal ini terjadi dikarenakan *Proxy* yang berjalan pada perusahaan baru dapat mengidentifikasi konten atau *category* yang diakses saja, untuk tindakan penjegahan masih harus melakukan *upgrade system proxy* yang digunakan.

Pengujian pada tahap ***actions on objectives***, mencoba untuk melakukan data *exfiltration* sebagai gambaran dari *action on objective* yang dilakukan *attacker*. Dengan menyalin data yang berukuran lebih dari 700Mb. Pertama dilakukan proses *copy* data kemudian mengekstraknya melalui protokol jaringan yang tidak terenkripsi menggunakan *Webdav*. Data juga dapat dikirim ke lokasi jaringan alternatif dari server *command and control*. Pengujian ini dapat dilihat pada Gambar 9 yang menunjukkan salah satu *server* telah berhasil di-*install webdav* dan attacker melakukan ekstraksi atau penyalinan data (proses *copy* data).

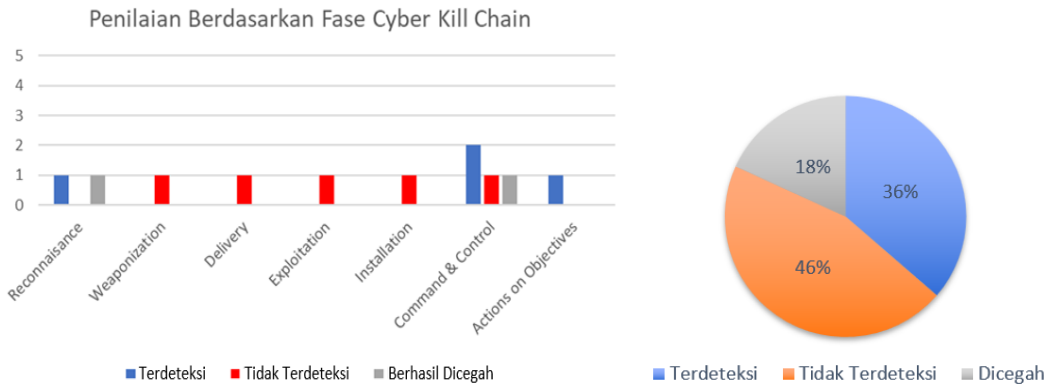


Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Contain*
☑	✗	✗	✗	✗	✗

Gambar 9. Pengujian Tahap *Actions on Objectives*

Dari percobaan yang dilakukan pada Gambar 9, teknologi keamanan perusahaan belum dapat mencegah aktivitas *data exfiltration* menggunakan *webdav*. Namun pada level deteksi upaya tersebut sudah dapat diketahui melalui teknology *proxy* yang digunakan.

Hasil dari setiap pengujian dirangkum untuk memudahkan dalam memahami celah keamanan yang dapat menjadi peluang bagi pihak yang tidak bertanggungjawab. Dapat dilihat pada Gambar 10.



(a) **(b)**

Gambar 10. (a) Rangkuman Hasil Pengujian, (b) Persentase Hasil Pengujian

Kelemahan Pada Sistem Keamanan Perusahaan

Beberapa kelemahan dalam sistem keamanan perusahaan yang perlu diperbaiki, yaitu:

1) Pada tahap *reconnaissance*, perusahaan telah melakukan beberapa tindakan pencegahan, namun masih ditemukan celah yang dapat dimanfaatkan oleh *attacker* seperti informasi yang dapat diperoleh melalui sumber publik.
2) Pada tahap *weaponization*, perusahaan belum memiliki tindakan pencegahan yang cukup baik, sehingga memungkinkan *attacker* untuk mengirimkan alat eksploitasi ke sistem target.
3) Hal yang sama juga terjadi pada tahap *delivery* dan *exploitation*, dimana perusahaan belum memiliki tindakan pencegahan yang memadai untuk mencegah serangan seperti pengiriman alat eksploitasi dan pengeksploitasian kerentanan pada sistem.
4) Pada tahap *installation*, perusahaan masih dapat melakukan deteksi, namun belum mampu melakukan tindakan pencegahan yang memadai untuk mencegah instalasi perangkat lunak atau kode berbahaya (jahat) pada sistem target.
5) Sedangkan pada tahap *command and control*, perusahaan dapat mendeteksi aktivitas, namun belum mampu melakukan tindakan pencegahan yang memadai untuk mencegah *attacker* mengontrol sistem.
6) Pada tahap *actions and objective*, perusahaan belum mampu melakukan tindakan pencegahan yang memadai untuk mencegah tindakan penyerangan seperti pencurian data dan penghancuran sistem.

Tindakan Mitigasi Berdasarkan Celah Keamanan

Perusahaan perlu melakukan pembaruan dan peningkatan keamanan pada sistem mereka untuk mencegah serangan siber di masa depan. Beberapa langkah yang dapat diambil oleh perusahaan, antara lain:

1) Menerapkan kebijakan keamanan yang lebih ketat, seperti pembaruan perangkat lunak yang rutin, penggunaan *firewall*, dan pelatihan kesadaran keamanan bagi karyawan.
2) Melakukan *upgrade* sistem *proxy* untuk meningkatkan kemampuan deteksi dan pencegahan serangan.
3) Menginvestasikan teknologi keamanan yang lebih canggih, seperti sistem deteksi intrusi dan pencegahan (*IDS* atau *IPS*), *sandboxing*, dan teknologi *threat intelligence*.
4) Melakukan audit keamanan secara berkala untuk mengidentifikasi dan memperbaiki celah keamanan yang ada.
5) Mengembangkan dan menguji rencana respon insiden untuk memastikan kesiapan organisasi dalam menghadapi serangan *cyber*.

KESIMPULAN

Pendekatan *Cyber Kill Chain Framework* yang dimanfaatkan pada penelitian ini menunjukkan bahwa pengelolaan keamanan infrastruktur dan sistem perusahaan. Beberapa hal telah berhasil dideteksi dengan baik, akan tetapi celah keamanan masih sangat terbuka ketika melihat pengujian yang dilakukan dan respon sistem keamanan perusahaan yang masih belum mengatasi dengan baik. Penelitian ini masih memiliki keterbatasan terkait dengan pengujian keamanan terhadap sistem perusahaan yang telah dilakukan. Dari penelitian ini dapat diketahui celah keamanan yang berhasil

diungkap masih belum kompleks. Akan tetapi tindakan komprehensif dari perusahaan masih belum siap terhadap skenario serangan yang dilakukan.

DAFTAR RUJUKAN

Abdul-Jabbar, S. S., Aldujaili, A., Mohammed, S. G., & Saeed, H. S. (2020). Integrity and security in cloud computing environment: a review. *Journal of Southwest Jiaotong University*, *55*(1). https://doi.org/10.35741/issn.0258-2724.55.1.11

Ahmed, Y., Asyhari, A. T., & Rahman, M. A. (2021). A cyber kill chain approach for detecting advanced persistent threats. *Computers, Materials and Continua*, *67*(2), 2497–2513. https://doi.org/10.32604/CMC.2021.014223

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, *2018*(5), 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Bollinadi, M., & Damera, V. K. (2017). Cloud computing: security issues and research challenges. *Journal of Network Communications and Emerging Technologies (JNCET) Www.Jncet.Org*, *7*(11). https://www.jncet.org/Manuscripts/Volume-7/Issue-11/Vol-7-issue-11-M-12.pdf

Capano, D. E. (2019). Understand the cyber-attack lifecycle: a cyber kill chain provides a model for understanding the lifecycle of a cyber attack and helps those involved with critical infrastructure improve cybersecurity policies, technologies, training, and industrial contr. *Control Engineering*, *66*(7), 32–34. https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=00108049&v=2.1&it=r&id=GALE%7CA597810215&sid=googleScholar&linkaccess=fulltext

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, *2018-Janua*, 4458–4466. https://doi.org/10.1109/BIGDATA.2017.8258485

Garba, F. A., Junaidu, S. B., Ahmad, B. I., & Tekanyi, A. M. S. (2019). Proposed framework for effective detection and prediction of advanced persistent threats based on the cyber kill chain. *Scientific and Practical Cyber Security Journal*, *3*(3). https://journal.scsa.ge/wp-content/uploads/2019/10/sept_2019_full_issue-n_c.pdf

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, *74*(10), 4986–5002. https://doi.org/10.1007/S11227-018-2337-2/TABLES/1

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/J.COMNET.2019.107094

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: a survey. *Computers 2014, Vol. 3, Pages 1-35*, *3*(1), 1–35. https://doi.org/10.3390/COMPUTERS3010001

Khidzir, N. Z., Mat Daud, K. A., Ismail, A. R., Abd. Ghani, M. S. A., & Ibrahim, M. A. H. (2018). Information security requirement: the relationship between cybersecurity risk confidentiality, integrity and availability in digital social media. *Regional Conference*

on Science, Technology and Social Sciences (RCSTSS 2016), 229–237. https://doi.org/10.1007/978-981-13-0074-5_21

Kiwia, D., Dehghantanha, A., Choo, K. K. R., & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Journal of Computational Science*, *27*, 394–409. https://doi.org/10.1016/J.JOCS.2017.10.020

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, 691–697. https://doi.org/10.1016/J.PROCS.2017.12.089

Lee, J.-S., Cho, S.-Y., Oh, H.-R., & Han, M.-M. (2021). A study on defense and attack model for cyber command control system based cyber kill chain. *Journal of Internet Computing and Services*, *22*(1), 41–50. https://doi.org/10.7472/JKSII.2021.22.1.41

Liu, W. (2012). Research on cloud computing security problem and strategy. *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 1216–1219. https://doi.org/10.1109/CECNET.2012.6202020

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, 125–138. https://doi.org/10.1016/J.IJCIP.2019.03.003

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *Journal of Supercomputing*, *76*(12), 9493–9532. https://doi.org/10.1007/S11227-020-03213-1/METRICS

Tchernykh, A., Schwiegelsohn, U., Talbi, E. ghazali, & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. https://doi.org/10.1016/J.JOCS.2016.11.011

Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access*, *6*, 25167–25177. https://doi.org/10.1109/ACCESS.2018.2817560

Wang, Y., Zhang, T., & Ye, Q. (2021). Situation awareness framework for industrial control system based on cyber kill chain. *MATEC Web of Conferences*, *336*, 02013. https://doi.org/10.1051/MATECCONF/202133602013

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/J.FUTURE.2010.12.006