AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

TUGAS AKHIR

Rudi Permana Yudha
41516110148

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2021

AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Rudi Permana Yudha
41516110148

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2021

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	: 41516110148
Nama	: Rudi Permana Yudha
Judul Tugas Akhir	: AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 16 Februari 2021

Rudi Permana Yudha

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Rudi Permana Yudha
NIM	:	41516110148
Judul Tugas Akhir	:	AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 16 Februari 2021

Rudi Permana Yudha

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Rudi Permana Yudha
NIM	:	41516110148
Judul Tugas Akhir	:	AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	√
		Jurnal Nasional Terakreditasi	√		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Teknik Informatika		
		ISSN	: eISSN : 25497901 | pISSN : 19799160		
		Link Jurnal	: http://journal.uinjkt.ac.id/index.php/ti/author/submission/19769		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 16 Februari 2021

Mengetahui
Dosen Pembimbing TA

Dwiki Jatikusumo, S. Kom.,M.Kom

Rudi Permana Yudha

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110148
Nama	:	Rudi Permana Yudha
Judul Tugas Akhir	:	AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 16 Februari 2021

TANDA TANGAN DIGITAL DOSEN PENGUJI

(Achmad Kodar, Drs. MT)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110148
Nama	:	Rudi Permana Yudha
Judul Tugas Akhir	:	AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 16 Februari 2021

(Diky Firdaus, S.Kom., MM)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110148
Nama	:	Rudi Permana Yudha
Judul Tugas Akhir	:	AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 16 Februari 2021

(Raka Yusuf, ST, MTI)

LEMBAR PENGESAHAN

NIM	:	41516110148
Nama	:	Rudi Permana Yudha
Judul Tugas Akhir	:	AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 16 Februari 2021

Menyetujui,

(Dwiki Jatikusumo, S. Kom..M.Kom)
Dosen Pembimbing

Mengetahui,

(Diky Firdaus. S.Kom. MM)	(Desi Ramayanti. S.Kom. MT)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Rudi Permana Yudha
NIM	:	41516110148
Pembimbing TA	:	Dwiki Jatikusumo, S. Kom.,M.Kom
Judul	:	Automasi Pengecekan Reputasi Sebuah IP Public Dengan Python

Kejahatan dunia maya semakin meningkat setiap tahun dan intensitas kerusakan juga meningkat, sehingga menimbulkan kewajiban tim cyber security organisasi untuk memperkuat cyber security, untuk menghindari kerugian yang besar bagi organisasi. Penggunaan daftar hitam publik adalah salah satu strategi untuk memperkuat keamanan jaringan organisasi guna mendeteksi komunikasi yang mencurigakan, namun, penggunaan daftar hitam publik menghasilkan persentase tinggi peringatan positif palsu dikarenakan memiliki sifat yang dinamis. oleh karenanya penulis mengimplementasikan Threat Intelligence Platform yang dapat memberikan indikator yang dapat diandalkan tentang ancaman siber dan merupakan sumber eksternal yang dibuat oleh komunitas atau entitas organisasi, yang melaporkan indikator yang mencurigai aktivitas berbahaya. Untuk mengurangi positif palsu administrator jaringan dapat melakukan pengecekan IP satu persatu setiap hari untuk memastikan IP tersebut apakah masih memiliki nilai reputasi yang tinggi atau tidak, sehingga akan memakan waktu yang lama dan kurang efisien. Pengecekan reputasi sebuah ip publik secara automasi menggunakan python adalah solusi untuk melakukan pekerjaan-pekerjaan yang rumit dan repetitif tersebut serta mengurangi peringatan positif palsu dan dengan dilakukan secara automasi dan dapat integrasikan dengan firewall untuk meningkatkan keamanan jaringan dari serangan siber dan metodologi penelitian yang akan digunakan adalah metodologi NDLC (Network Development Life Cycle).

Kata kunci:
Kejahatan Siber, daftar hitam public IP, Threat Intelligence, Automasi dan Reputasi IP Publik

ABSTRACT

Name	:	Rudi Permana Yudha
Student Number	:	41516110148
Counsellor	:	Dwiki Jatikusumo, S. Kom.,M.Kom
Title	:	Automasi Pengecekan Reputasi Sebuah IP Public Dengan Python

Cybercrimes are getting increased every year and the intensity of damage is also increasing, hence it raises the obligation of the organization's cybersecurity team to strengthen the cybersecurity, to avoid losses to the organization. Although the use of public blacklists reinforces the cyber security by monitoring the organization network communication, the use data from IP blacklists generates a high percentage of false positives alerts because it's dynamic. Therefore the authors implement a threat intelligence platform that can provide reliable indicators of cyber threats and is an external source created by a community or organizational entity, which reports indicator that suspect malicious activity. To reduce false positives administrators can do manuals to check IPs one by one every day to ensure that the IP still has a high reputation value or not, so it will take a long time and be less efficient. Checking the reputation of a public ip in automation using python is a solution to do these complex and repetitive jobs and reduce false positive alerts and by automating it can integrate with firewalls to increase network security from cyber attack and research methodology that will be used is the methodology of NDLC (Network Development Life Cycle).

Key words:
Cybercrime, Public IP Blacklist, Threat Intelligence, Automation and IP Public Reputation

KATA PENGANTAR

Puji syukur kita panjatkan kehadiratnya Allah SWT, atas limpahan Rahmat dan Karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul : Automasi Pengecekan Reputasi Sebuah IP Public Dengan Python untuk memenuhi salah satu syarat menyelesaikan studi serta dalam rangka memperoleh gelar Sarjana Pendidikan Strata Satu pada Program Studi Teknik Informatika Fakultas Ilmu Kmputer Universitas Mercubuana Jakarta. Dalam penulisan tigas akhir ini , tentunya banyak pihak yang telah memberikan bantuan baik moral maupun meteril. Oleh karena itu penulis ingin menyampaikan banyak ucapan terimakasih kepada :

1. Allah SWT dengan segala rahmat serta karunia-Nya yang memberikan kekuatan bagi peneliti dalam menyelesaikan tugas akhir ini.
2. Kepada kedua orang tua tercinta yang selama ini telah membantu peneliti dalam bentuk perhatian, kasih sayang, semangat, serta doa yang tidak hentihentinya mengalir demi kelancaran dan kesuksesan peneliti dalam menyelesaikan skripsi ini.
3. Kepada Istri tercinta Riska Rosmayanti yang selalu mensupport dan mendoakan demi kelancaran dan kesuksesan peneliti dalam menyelesaikan skripsi ini.
4. Kepada Anak tercinta Hafsah Nadira Salwa yang menjadikan semangat untuk cepat menyelesaikan skripsi ini.
5. Bapak Anis Cherid, SE, MTI selaku dosen Pembimbing Akademik.
6. Bapak Dwiki Jatikusumo, S. Kom.,M.Kom Dosen Pembimbing tugas akhir.
7. Ibu Desi Ramayanti, S.Kom, MT selaku Ka.Prodi informatika.
8. Bapak Dr. Mujiono ST,MTI selaku Dekan FASILKOM.
9. Teman-teman satu angkatan yang selalu menyemagati baik dalam perkuliahan dan pembuatan tugas akhir.

Jakarta, 16 Februari 2021

Rudi Permana Yudha

DAFTAR ISI

NASKAH JURNAL

AUTOMASI PENGECEKAN REPUTASI SEBUAH IP PUBLIC DENGAN PYTHON

Rudi Permana Yudha[1], Dwiki Jatikusumo[2]

[1,2]Teknik Informatika, Fakultas Ilmu Komputer
Universitas Mercu Buana
Jl. Meruya Selatan No. 1, Kembangan, Jakarta Barat, Indonesia 11650
[1]41516110148@student.mercubuana.ac.id, [2]dwiki.jatikusumo@mercubuana.ac.id

ABSTRACT

Cybercrimes are getting increased every year and the intensity of damage is also increasing, hence it raises the obligation of the organization's cybersecurity team to strengthen the cybersecurity, to avoid losses to the organization. Although the use of public blacklists reinforces the cyber security by monitoring the organization network communication, the use data from IP blacklists generates a high percentage of false positives alerts because it's dynamic. Therefore the authors implement a threat intelligence platform that can provide reliable indicators of cyber threats and is an external source created by a community or organizational entity, which reports indicator that suspect malicious activity. To reduce false positives administrators can do manuals to check IPs one by one every day to ensure that the IP still has a high reputation value or not, so it will take a long time and be less efficient. Checking the reputation of a public ip in automation using python is a solution to do these complex and repetitive jobs and reduce false positive alerts and by automating it can integrate with firewalls to increase network security from cyber attack and research methodology that will be used is the methodology of NDLC (Network Development Life Cycle).

Keywords: *Cybercrime, Public IP Blacklist, Threat Intelligence, Automation and IP Public Reputation*

ABSTRAK

Kejahatan dunia maya semakin meningkat setiap tahun dan intensitas kerusakan juga meningkat, sehingga menimbulkan kewajiban tim *cyber security* organisasi untuk memperkuat *cyber security*, untuk menghindari kerugian yang besar bagi organisasi. Penggunaan daftar hitam publik adalah salah satu strategi untuk memperkuat keamanan jaringan organisasi guna mendeteksi komunikasi yang mencurigakan, namun, penggunaan daftar hitam publik menghasilkan persentase tinggi peringatan positif palsu dikarenakan memiliki sifat yang dinamis. oleh karenanya penulis mengimplementasikan *Threat Intelligence Platform* yang dapat memberikan indikator yang dapat diandalkan tentang ancaman siber dan merupakan sumber eksternal yang dibuat oleh komunitas atau entitas organisasi, yang melaporkan indikator yang mencurigai aktivitas berbahaya. Untuk mengurangi positif palsu administrator jaringan dapat melakukan pengecekan IP satu persatu setiap hari untuk memastikan IP tersebut apakah masih memiliki nilai reputasi yang tinggi atau tidak, sehingga akan memakan waktu yang lama dan kurang efisien. Pengecekan reputasi sebuah ip publik secara automasi menggunakan python adalah solusi untuk melakukan pekerjaan-pekerjaan yang rumit dan repetitif tersebut serta mengurangi peringatan positif palsu dan dengan dilakukan secara automasi dan dapat integrasikan dengan *firewall* untuk meningkatkan keamanan jaringan dari serangan siber dan metodologi penelitian yang akan digunakan adalah metodologi NDLC (Network Development Life Cycle).

Kata Kunci: *Kejahatan Siber, daftar hitam public IP, Threat Intelligence, Automasi dan Reputasi IP Publik*

I. PENDAHULUAN

Meningkatnya insiden kejahatan dunia maya yang terjadi di dunia berada pada tingkat yang membahayakan yang menyebabkan kerugian bisnis yang sangat besar yang diakibatkan oleh serangan ini, termasuk dalam hal uang, produktivitas, reputasi dan kepercayaan terhadap teknologi[1], [2]. *Threat Intelligence* (TI) adalah proses penggalian informasi tentang ancaman dunia maya dari beragam sumber, internal dan eksternal hingga organisasi. Ini adalah daftar yang dibuat oleh komunitas atau entitas organisasi, yang melaporkan informasi yang mencurigai aktivitas berbahaya[3]. Sumber-sumber informasi keamanan siber internet dapat memberikan indikator yang dapat diandalkan tentang ancaman siber seperti misalnya, daftar hitam IP publik, *File Hash* dan Uniform Resource Locators (URL)[4].

Threat Intelligence tersedia gratis maupun komersial baik sebagai penyedia data atau sebagai sistem yang dapat memberikan penilaian terhadap suatu indikator ancaman, seperti IBM X-FORCE, FS-ISAC dan lainnya[5]. Untuk mendapatkan data dari *Threat Intelligence Platform* dibutuhkan client untuk berkomunikasi dan menampung data yang support dengan protokol STIX/TAXII[6]. *Threat Intelligence* digunakan untuk mendapatkan indikator ancaman dalam hali ini contohnya *blacklist* IP yang kemudian di gunakan untuk meningkatkan keamanan jaringan, namun dikarenakan tidak adanya pengecekan reputasi IP secara berkala mengakibatkan tingginya peringatan positif palsu dikarenakan memiliki sifat dinamis[7].

Firewall ada perangkat keamanan yang berfungsi untuk melindungi jaringan computer yang menciptakan penghalang antara jaringan terpercaya dan jaringan tidak terpercaya[8]. Python dikenal sebagai bahasa untuk pemrograman tujuan umum, dan saat ini digunakan dalam banyak bidang, seperti pengembangan perangkat lunak, pengembangan web, otomatisasi, administrasi sistem, dan bidang ilmiah. Berkat banyaknya modul yang tersedia untuk diunduh, mencakup banyak bidang, Python dapat mengurangi waktu pengembangan hingga seminimal mungkin[9]. Dalam pengembangan API diperlukan sebuah gaya arsitektur sebagai pedoman cara berhubungan antara logic basis data dengan logic antarmuka. Salah satu gaya arsitektur pengembangan API berbasis web yang menggunakan HTTP dalam komunikasi data adalah *Representational State Transfer* (REST)[10].

Setelah mengetahui serta mencari informasi yang telah dipaparkan berdasarkan hal-hal tersebut maka penulis bermaksud untuk menggunakan *Open Threat Intelligence Platform* untuk mendapatkan *Blacklist* IP yang kemudian *list* tersebut di maintain data tersebut secara regularly melakukan pengecekan nilai reputasi secara automasi menggunakan Python dan REST API selanjutnya dapat digunakan firewall untuk meningkatkan keamanan jaringan.

II. METODOLOGI

Metode pengumpulan data dan informasi yang digunakan dalam penelitian ini adalah mengumpulkan bahan-bahan yang didapat dari buku-buku, jurnal, studi lapangan serta analisis desain dan kebutuhan sistem. Dalam pembuatan sistem ini menggunakan metode NDLC (Network Development Life Cycle) [11] yang terdiri dari 6 tahap namun dalam penelitian ini hanya menggunakan 5 tahapan yaitu Analysis, Design, Implementation, Monitoring dan Management.

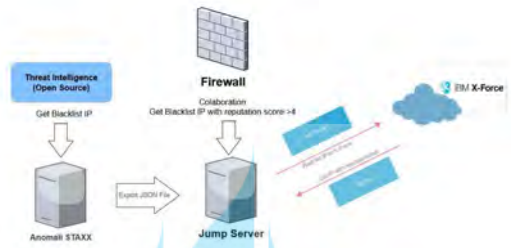
1. Analysis

Tahap awal peniliti melakukan analisa permasalahan yang muncul. Sistem ini dibuat untuk melakukan pengumpulan blacklist IP dari berbagai *Open Threat Intelligence Platform*, yang kemudian akan dilakukan *maintaining* blacklist IP secara automasi menggunakan Python dan REST API pada Jump Server. Disini peneliti menggunakan Anomali STAXX [12] sebagai *Threat Intelligence Feed* atau media untuk mengambil data dari *Threat Intelligence Platform* dan IBM X-Force [13] sebagai komersial *Threat Intelligence Platform* untuk mendapatkan nilai reputasi dari indikator ancaman yang sebelumnya didapatkan dari *Open Threat Intelligence.* Pada Gambar 1 menjelaskan skema dari sistem yang akan di buat.

Gambar 1. Skema System

2. Design

Dalam tahap desain yaitu membuat *flow* untuk menggambarkan cara kerja dari sistem



Gambar 2. Topologi

3. Implementasi

Pada tahap implementasi ini menerapkan semua yang sudah disiapkan dan direncanakan dengan mengacu pada tahap desain yang telah dirancang. Ruang lingkup tahapan ini yaitu :

a. Membangun server Anomali STAXX [14]
b. Membangun jump server dengan OS Centos 7, menginstall aplikasi dan library yang dibutuhkan sebagaimana tertera pada tabel 1.

Tabel 1. Spesifikasi *Software* dan *Library*

Software	***Library***
Python 3	certifi chardet idna requests urllib3
HTTPD	

c. Membuat script automation
d. Menjalankan script untuk mendapatkan Blacklist IP
e. Membangun Firewall dan Integrasi dengan Blacklist IP

4. Monitoring

Tahap ini merupakan tahap yang penting agar script dapat berjalan sesuai dengan keinginan dan tujuan seperti pada tahap awal analisis.

5. Management

Melakukan pemeliharaan pada system threat intelligence dan jump sever dengan memastikan kapasitas storage dan koneksi jaringan berfungsi dengan semestinya.

III. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini dibagi menjadi tiga bagian. Pertama mendapatkan blacklist IP dari Threat Intelligence, Kedua membuat *script* automasi dengan Python dan REST API dan Ketiga mengintegrasikan blacklist IP dengan firewall.

3.1 Mendapatkan *Blacklist* IP

Pada tahap ini pengujian dilakukan dengan melakukan konfigurasi pada Anomali STAXX, dimana kita akan menambahkan *Threat Intelligence Platform* agar mendapatkan Blacklist IP. Sebelumnya kita harus mempunyai user dan password terlebih dahulu untuk terhubung dengan *Threat Intelligence Platform*. Di sini kita menggunakan 2 sumber yaitu https://limo.anomali.com/taxii/ dan https://threatfeed.cyware.com/ctixapi/taxii/ dan apabila konfigurasi sudah benar maka akan menampilkan status *complated* pada bagian discovery seperti pada gambar 4 dan daftar ip sudah muncul seperti gambar 5.

Gambar 3. Halaman login Anomali STAXX

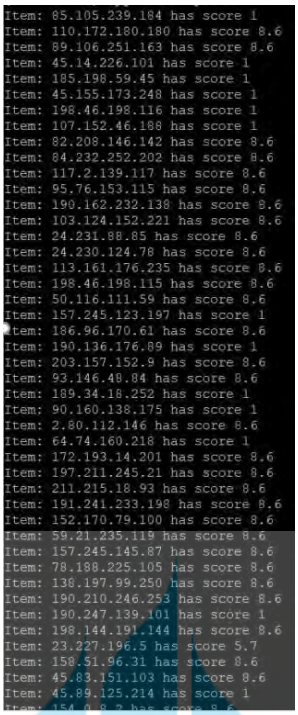
Gambar 4. Konfigurasi Site

Gambar 5. Halaman Melihat Daftat IP

3.2 Menjalankan *Script* Automasi

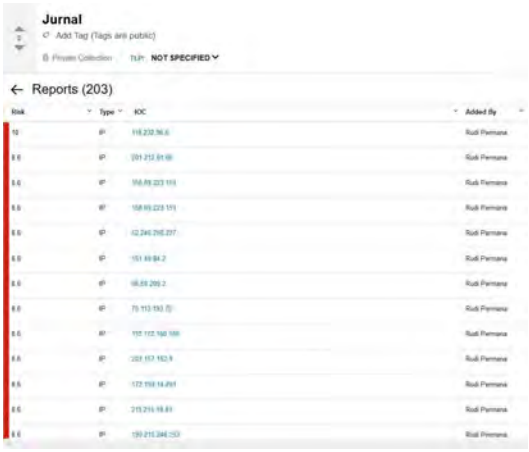
Pada tahap ini peneliti menjalankan *script* automasi yang telah dibuat untuk melakukan pengecekan reputasi IP yang didapatkan dari Anomali STAXX ke IBM X-FORCE *Threat Intelligence Platform* menggunakan bahasa pemrograman Python dan REST API pada jump server.

Bagaimana proses pengecekan reputasi IP yang dilakukan script dapat di lihat pada gambar 6 dan untuk melihat hasil IP dengan nilai reputasi >4 dapat merujuk pada gambar 7 serta komparasi data dari IBM X-Force jika dilakukan manual pengecekan dapat merujut pada Gambar 8. Selanjutnya script akan dijalankan secara automasi pada background proses mengikuti jadwal yang telah ditentukan yaitu setiap hari pada pukul 00.00.



Gambar 6. Contoh proses saat script dijalankan

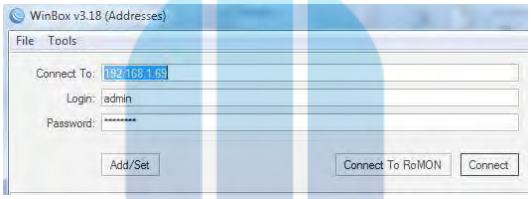
Gambar 7. Isi file dari hasil pengecekan reputasi



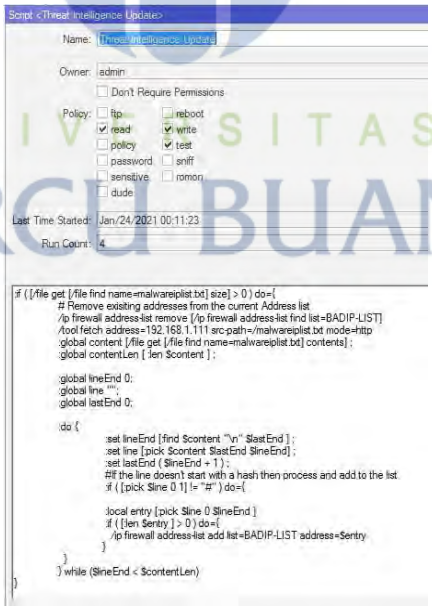
Gambar 8. Komparasi data pada IBM X-Force

3.3 Integrasi *Blacklist* IP dengan Firewall

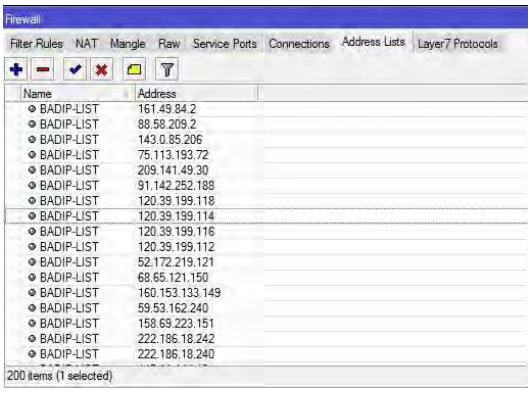
Pada tahap ini peneliti melakukan konfigurasi pada *firewall* untuk mengambil data *file blacklist* yang berada di jump server secara automasi menggunakan scheduler yang berjalan setiap hari pada jam 6 pagi. Pertama kita login ke firewall menggunakan winbox seperti pada Gambar 9, kemudian membuat script seperti pada Gambar 10, kemudian setelah script dijalankan akan menghasilkan *list* ip seperti pada Gambar 11.



Gambar 9. Halaman login firewall (mikrotik)



Gambar 10. *Script Blacklist* IP



Gambar 11. *List* IP *Firewall*

IV. PENUTUP

Berdasarkan data yang diperoleh serta analisis yang sudah dilakukan dari penelitian Automasi Pengecekan Reputasi Sebuah IP Public Dengan Python yang telah dilakukan ini maka dapat diambil kesimpulan sebagai berikut:

1. Pengecekan reputasi dari daftar IP yang diperoleh dari Anomali STAXX dapat berjalan secara otomatis sehingga mengurangi terjadinya peringatan positif palsu.
2. Reputasi IP publik pada *blacklist* IP hanya berisi IP dengan nilai reputasi dengan resiko tinggi
3. Meningkatkan proteksi dari serangan siber dengan sudah diblock nya komunikasi dari jaringan internal ke IP dengan reputasi buruk ataupun sebaliknya pada perangkat keamanan (*firewall*).

DAFTAR PUSTAKA

[1] T. U. D. of Justice, "How to protect your networks from Ransomware," p. 9, 2016, [Online]. Available: https://www.justice.gov/criminal-ccips/file/872771/download.

[2] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives," *13th Int. Conf. Wirtschaftsinformatik*, pp. 837–851, 2017.

[3] M. Bromiley, "Information Security Reading Room Threat Intelligence : What It Is , and How to Use It _____ Threat Intelligence : What It Is , and How to Use It Effectively," 2021.

[4] N. S. Agency and C. Information, "Integrate Threat Reputation Services," no. August, pp. 1–4, 2019.

[5] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence – Issue and challenges," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 1, pp. 371–379, 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.

[6] G. Wang, Y. Huo, and Z. M. Ma, "Research on University's Cyber Threat Intelligence Sharing Platform Based on New Types of STIX and TAXII Standards," *J. Inf. Secur.*, vol. 10, no. 04, pp. 263–277, 2019, doi: 10.4236/jis.2019.104015.

[7] J. Alves, A. Respício, A. Lasige, ; B Cmafio, I. Rosa, and P. Rodrigues, "Threat Intelligence Improving SIEM cybercriminality awareness using information from IP blacklists," *ymposium Electron. Crime Res.*, 2017, [Online]. Available: https://www.justice.gov/criminal-ccips/file/872771/download.

[8] M. Imran, A. A. Alghamdi, and B. Ahmad, "Role of firewall Technology in Network Security," *Int. J. Innov. Adv. Comput. Sci.*, no. December 2015, pp. 3–6, 2015.

[9] Bassem Aly, *Hands-On Enterprise Automation with Python*. Packt Publishing, 2018.

[10] B. Adi Pranata, A. Hijriani, and A. Junaidi, "Perancangan Application Programming Interface (Api) Berbasis Web Menggunakan Gaya Arsitektur Representational State Transfer (Rest) Untuk Pengembangan Sistem Informasi Administrasi Pasien Klinik Perawatan Kulit," *J. Komputasi*, vol. 6, no. 1, pp. 33–42, 2018, doi: 10.23960/komputasi.v6i1.1554.

[11] M. Syani and A. M. Ropi, "Analisis Dan Implementasi Network Security System Menggunakan Teknik Host-Based Intrusion Detection System (Hids) Berbasis Cloud Computing," *Semin. Nas. Telekomun. dan Inform. (SELISIK 2018)*, no. September, p. 2, 2018.

[12] A. de Melo e Silva, J. J. C. Gondim, R. de Oliveira Albuquerque, and L. J. G. Villalba, “A methodology to evaluate standards and platforms within cyber threat intelligence,” *Futur. Internet*, vol. 12, no. 6, pp. 1–23, 2020, doi: 10.3390/fi12060108.
[13] IBM *et al.*, “X-Force Threat Intelligence Index 2020,” *IBM X-Force Incid. Response Intell. Serv.*, p. 49, 2020, [Online]. Available: https://www.ibm.com/downloads/cas/DEDOLR3W.
[14] Anomali. Anomali STAXX—Installation andAdministrationGuide. 2018. Available online: https://update.anomali. com/staxx/docs/Anomali_STAXX_Installation_&_Administration_Guide.pdf (accessed on 20 Dec 2020)

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul di atas. Kertas kerja berisi semua material hasil penelitan Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan:

1. literature review
2. Hasil analisa & perancangan aplikasi
3. Source Code
4. Tahapan eksperimen

Hasil eksperimen secara keseluruhan