ANALISIS KEAMANAN JARINGAN MIKROTIK ISP INDONESIA MENGGUNAKAN SEARCH ENGINE SCADA SHODAN DENGAN METODE EXPLOIT WINBOX CRITICAL VULNERABILITY

Julianto[1], Suwanto Raharjo[2], Catur Iswahyudi[3]

[1,2,3]Jurusan Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email:[1]antoaja1780@gmail.com, [2]wa2n@akprind.ac.id, [3]catur@akprind.ac.id

ABSTRACT

Mikrotik is very familiar to internet users in Indonesia as an operating system and software that can be used to turn an ordinary computer into a network router. Besides that, the problems that often occur on Mikrotik routers on the user side do not increase the Mikrotik version which has a v6.42-v6.28 Mikrotik vulnerability so that it is easy to exploit. This study aims to analyze the security system for access to the proxy router and to do mitigation or prevention and security solutions from Exploit attacks. The method used in this research is using experimental methods, literature study and simulation. In conducting trials, this study uses the Exploit Winbox critical vulnerability technique against Mikrotik devices which are known to still have security holes by utilizing the Scada Shodan search engine as a public Ip searcher from Mikrotik. The results of the research carried out are concluding and providing solutions on how to overcome and prevent re-attacks on the security problem of proxy router access from exploit attacks, in this case it can be a consideration for IT security agencies or companies to secure the proxy router from exploit attacks.

Keywords: *Microtik, shodan, and exploit vulnerabilities.*

INTISARI

Mikrotik sudah sangat familiar bagi pengguna internet di Indonesia sebagai sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network. Disamping itu masalah yang sering terjadi pada router mikrotik terhadap sisi pengguna tidak meningkatkan versi mikrotik yang memiliki celah kerentanan mikrotik v6.42-v6.28 sehingga mudah diexploit. Penelitian ini bertujuan untuk menganalisis sistem keamanan akses router mikrotik serta melakukan cara mitigasi atau pencegahan dan solusi keamanan dari serangan Exploit. Metode yang digunakan dalam penelitian ini menggunakan metode eksperimen, studi pustaka dan simulasi. Dalam melakukan ujicoba, penelitian ini menggunakan teknik Exploit winbox critical vulnerability terhadap perangkat mikrotik yang diketahui masih memiliki celah keamanan dengan memanfaatkan search engine scada shodan sebagai pencari Ip publik dari mikrotik. Hasil dari penelitian yang dilakukan yaitu menyimpulkan dan memberikan solusi bagaimana cara menanggulangi dan mencegah kembali serangan terhadap masalah keamanan akses router mikrotik dari serangan exploit dalam hal ini bisa menjadi bahan pertimbangan bagi IT security instansi atau perusahaan untuk mengamankan router mikrotik dari serangan exploit.

Kata Kunci: Kerentanan mikrotik, shodan dan exploit.

PENDAHULUAN

Mikrotik telah lama dikenal sebagai sistem operasi dan perngkat lunak yang mampu menjadikan computer berfungsi sebagai router jaringan. Sebagai penyedia solusi murah untuk fungsi router tidak heran jika pengguna mikrotik di Indonesia cukup besar terutama dipulau Jawa dan Bali. Jadi sudah sepatutnya pengguna di Indonesia lebih berhati-hati, mengingat jumlah

mikrotik yang berhasil disusupi tercatat lebih dari 200.000 penyusupan terjadi dalam dunia internet (autotekno, 2018). Sebagai penyedia solusi murah untuk fungsi router, jumlah pengguna mikrotik di Indonesia sangat besar yaitu 127.096 (shodan, 2009). Para peretas keamanan sistem informasi menerapkan metode atau teknik-teknik dalam melakukan penyerangan suatu sistem. Exploit merupakan salah satu teknik yang sering digunakan para peretas untuk menyerang keamanan sebuah sistem. Exploit adalah sebuah kode atau sekumpulan kode, ataupun program yang mengandung kode-kode yang menyerang sisi kelemahan dari sebuah sistem yang telah dibuat (Chandra, dkk, 2016). Efek dari serangan teknik Exploit tersebut dapat bermacam-macam dari sisi pengguna pribadi yaitu kehilangan informasi pribadi menyangkut pengguna sistem, karna informasi yang didapatkan oleh peretas biasa digunakan untuk hal yang illegal.

Keamanan telah menjadi aspek penting bagi dunia internet, layanan dalam sebuah server harus memiliki tingkat keamanan yang terjamin, agar layanan hanya dapat diakses oleh orang yang berhak untuk mengakses layanan tersebut. Keamanan server saat ini sangat penting karena menyangkut privasi seseorang maupun privasi sebuah lembaga atau perusahaan, tidak hanya peretasan kini para pengguna router mikrotik juga mendapat beberapa macam insiden yang dapat merugikan personal, lembaga, isp, maupun perusahaan insiden tersebut dapat digolongkan menjadi tiga bagian utama yaitu *vulnerabilities*, *attacks* dan *viruses*. Mengukur tingkat keamanan sebuah server dapat dilakukan dengan berbagai cara diantaranya dengan menggunakan dua metode penilaian kerentanan dan pengujian penetrasi (Santoso, 2019).

Pada awal tahun 2018 *Czech technology* forum melaporkan adanya indikasi serangan *zero-day attack* terhadap akses router mikrotik serangan ini menargetkan winbox pada router mikrotik sebelum versi 6.42. Serangan ini memodifikasi permintaan *request* untuk mengubah satu *byte* yang terkait dengan *session* ID pada winbox mikrotik routerOS sehingga dapat mengambil alih akses router mikrotik. Setelah dilakukan investigasi lebih lanjut ditemukan bukti bahwa kerentanan mikrotik memiliki celah kerentanan CVE-2018-14847 untuk mendapatkan akses kedalam router mikrotik. Memungkinkan penyerang mengeksploitasi winbox melalui port 8291, setelah melakukan eksploitasi penyerang bisa masuk ke dalam router mikrotik sebagai admin, bahaya dari serangan eksploitasi ini penyerang bisa menanam virus atau memanpatkan ip publik sebagai vpn dan mengambil data-data dari pengguna seperti user dan password hotspot (bssn, 2018).

Berdasarkan penjelasan dalam latar belakang tersebut, sangat penting untuk mengetahui bagaimana cara mencegah serangan exploit, dan mengatasi sistem yang terdapat kelemahan dalam router mikrotik. Tujuan penelitian ini adalah Analisis Keamanan Jaringan Mikrotik Isp Indonesia Menggunakan *Search Engine Scada Shodan* Menggunakan Exploit *Winbox Critical Vulnerability*".

Beberapa penelitian terdahulu yang berkaitan dengan penelitian ini adalah penelitian yang dilakukan oleh Arta, dkk, (2018) menyebutkan bahwa dibutuhkan sebuah sistem yang dapat membantu network administrator untuk digunakan sebagai monitor trafik jaringan dengan IPS yang merupakan kombinasi antara fasilitas *blocking capabilities* dari *Firewall*. Metode yang digunakan yaitu analisis, perancangan, pengujian dan dokumentasi. Hasil penelitian serangan atau penyusupan yang terjadi pada suatu system, serangan biasanya pengguna menggunakan *bruteforce* untuk mendapatkan *username* dan *password*, serangan yang dilakukan dengan Nmap untuk mendeteksi port IP apa saja yang terbuka dapat dicegah atau dideteksi menggunakan ruleIPS.

Prayudi & Putro (2018) menyebutkan bahwa dalam sebuah aktifitas jaringan dibutuhkan monitoring alur akses data yang mencurigakan dapat teratasi sebelum hal yang tidak didingnkan terjadi. Untuk itu penulis mengharapkan dalam penelitian ini teknologi metarouter selain dimanfaatkan untuk menghemat juga dikembangkan untuk manajemen dan keamanan data dalam sebuah jaringan komputer dengan metode simulasi monitoring trafik. Hasil dari penelitian ini dengan metarouter dapat menjalankan beberapa routerOS dalam menerapakan simulasi keamanan dari serangan *Dos*.

Dalam penelitian ini telah dilakukan penelitian untuk mengembangkan keamanan jaringan komputer dengan metode Port *Knocking*. Berdasarkan penelitian yang telah dilakukan (Amarudin 2018) simulator GNS3 dapat dengan mudah diterapkan dalam mendesain topologi jaringan maupun dalam mensimulasikan pengujian keamanan jaringan khususnya pada metode keamanan Port *Knocking*.

Penerapan desain firewall terhadap serangan ddos pada router mikrotik, serangan DDoS atau UDP Flood dapat merugikan dari sisi perangkat lunak dan perangkat keras. Hasil dari

penelitian dengan adanya suatu konfigurasi didalam router mikrotik dapat mencegah serangan dari pihak luar yang menggunakan serangan DDoS, dan dapat mencegah terjadinya jaringan troubleshooting sehingga jaringan lebih secure dan lebih baik. (Shaifullah, 2019).

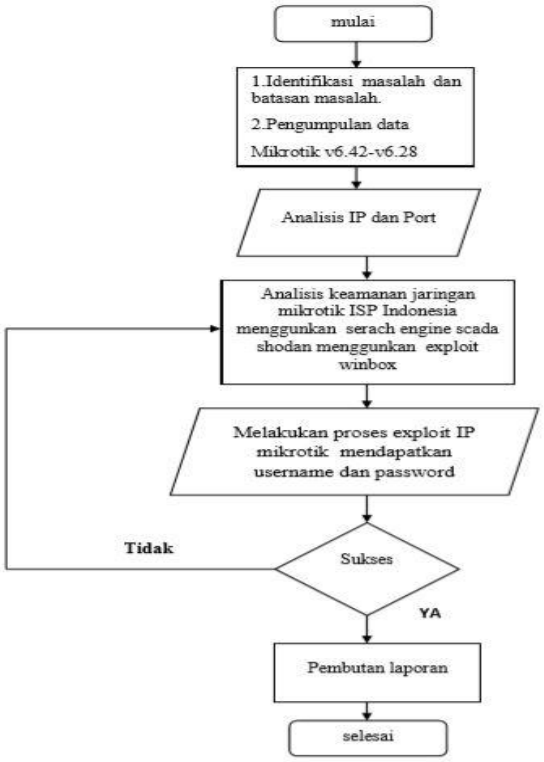
Penerapan analisis dan perancangan keamanan akses router mikrotik dari serangan exploit, bertujuan untuk menganalisis sistem keamanan akses router mikrotik serta melakukan cara mitigasi atau pencegahan dan solusi keamanan dari serangan exploit. Hasil dari penelitian yang dilakukan yaitu menyimpulkan dan memberikan solusi bagaimana cara menanggulangi dan mencegah kembali serangan terhadap masalah keamanan akses router mikrotik dari serangan exploit, dalam hal ini bisa menjadi bahan pertimbangan bagi IT *security* di instansi atau perusahaan untuk mengamankan router mikrotik dari serangan exploit. (Khayudi, 2019).

.

METODOLOGI PENELITIAN

Diagram Alir Penelitian

Diagram alir langkah penelitian dalam Analisis Keamanan Jaringan Mikrotik ISP Indonesia menggunakan *Search Engine Scada Shodan* Menggunakan Exploit *Winbox Critical Vulnerability.*



Gambar 1. . Diagram Alir penelitian

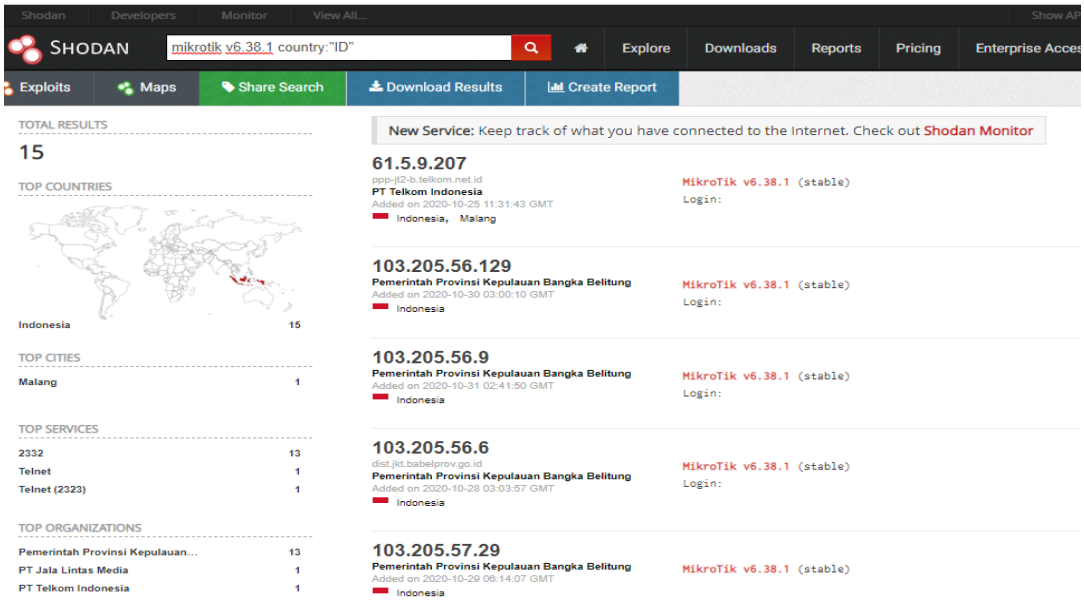
Langkah yang dilakukan dalam penelitian ini berupa diagram alir. Tahap pertama melakukan persiapan terhadap penelitian yang akan dilakukan menyiapkan data-data atau sampel berupa IP publik dari berbagai IP diseluruh Indonesia, yang didapatka dari *search engine shodan* yang memindai semua perangkat yang terhubung ke internet IP yang sudah didapatkan dijadikan sebagai objek exploit. Selanjutnya tahap pencarian IP pubik ISP yang masih menggunakan versi mikrotik v6.42-v6.28 yang akan dicari melauli *search engine shodan* setelah mendapatkan IP publik dari berbagai ISP yang akan diexploit. Tahap berikutnya yaitu tahap analisis port IP publik yang sudah didaptakan dari *search engine shodan,* dimana terlebih dahulu menganalisis port apa saja yang terbuka dalam IP yang sudah didapatkan selajutnya *tools* yang digunkan untuk mencari port yang terbuka menggunakan Zenmap dimana *tools* Zenmap akan menganalisis port yang terbuka baik port yang difilter atau ditutup. Jika port yang difilter tertutup maka proses exploit tidak bisa dilakukan. Langkah selanjutnya yaitu melakukan peroses exploit dengan *Winbox Critical vulnerability* untuk proses implementasi dari IP publik yang sudah didaptakan untuk proses exploit IP publik mikrotik untuk mendapatkan *username* dan *password* dari mikrotik, jika proses exploit

tidak berjalan maka IP publik yang diexploit memliki filter port yang sudah diblok maka akan kembali ke langkah analisis port, dan jika proses exploit berjalan maka akan menampilakan *username* dan *password* dari router admin maka akan dilanjutkan ke proses pembuatan laporan.

HASIL DAN PEMBAHASAN

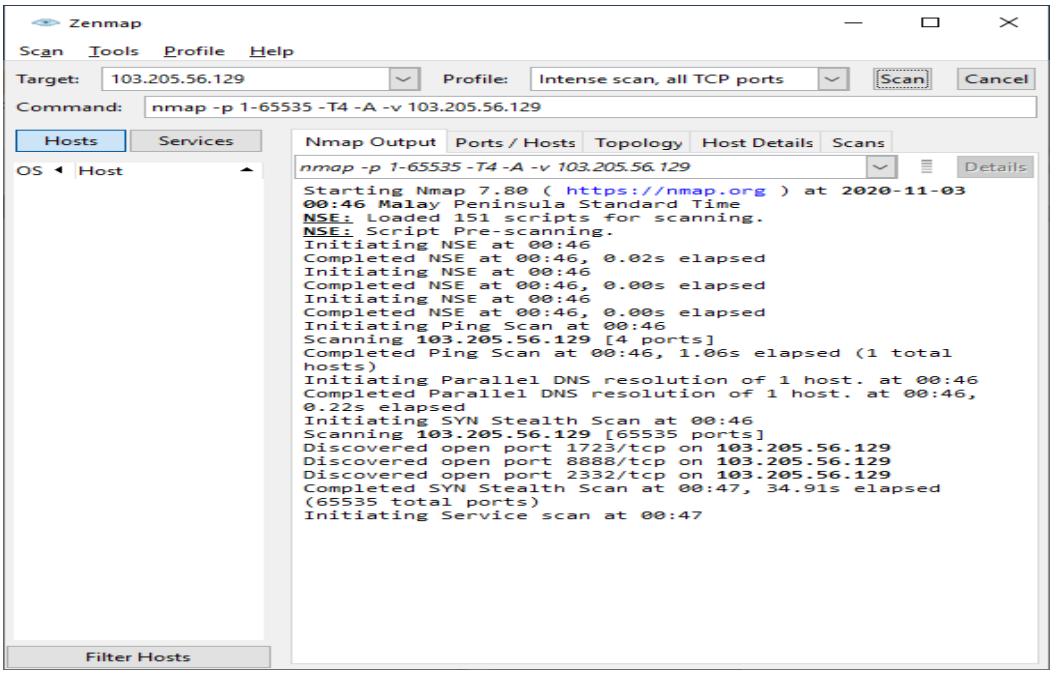
Hasil Penelitian

Shodan adalah mesin pencari pertama didunia untuk perangkat yang terhubung ke internet, shodan juga bisa menemukan perangkat yang terhubung ke internet, dimana lokasinya, dan siapa yang menggunakannya. Shodan bisa melacak semua komputer dijaringan yang dapat diakses langsung dari internet Tampilan halaman utama pencarian IP publik dengan web shodan dan versi mikrotik yang rentan v6.42-v6.28 yang dapat di cari menggunakan shodan Ditunjukan pada Gambar 2.



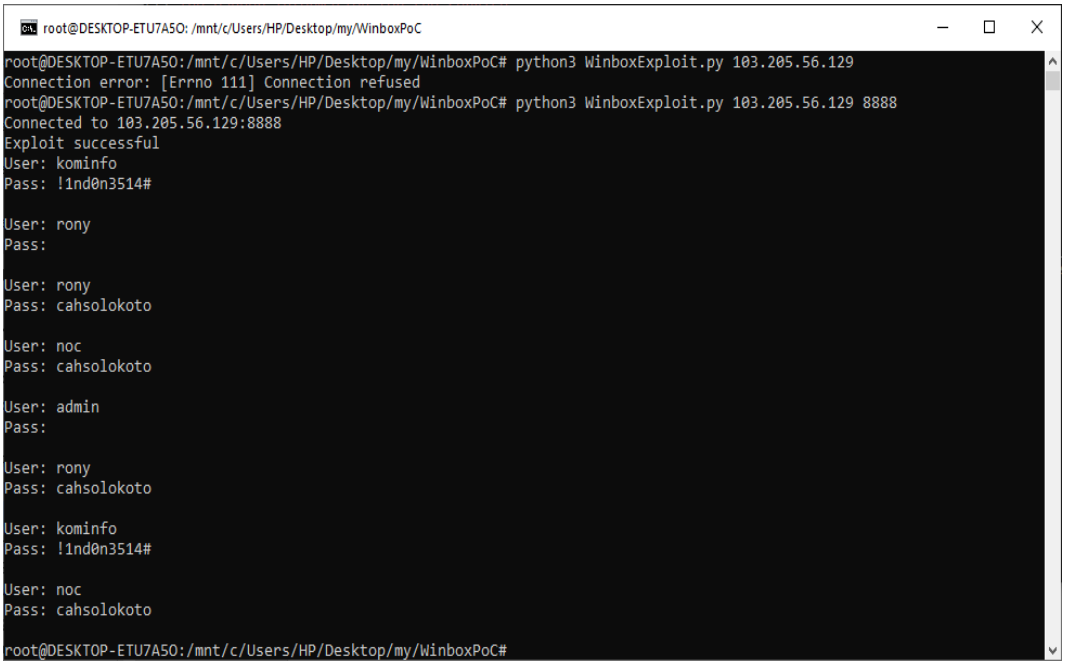
Gambar 2. . Search IP publik menggunakan web shodan

Tampilan halaman analisis IP publik port mikrotik menggunakan zenmap hasil analisis IP publik mikrotik menggunakan Zenmap untuk melakukan pencarian port apa saja yang terbuka setelah melakukan scan terdapat beberapa data. dari hasil Scanning IP publik port yang terbuka setelah dianalisis terdapat 3 port, dan 1 host jika host 0 maka port tidak bisa dipakai, untuk proses exploit biasanya port default winbox 8291, setelah di scanning atau dianalisis ternyata port dari router mikrotik adalah port 8888, ditahap selanjutnya bisa melakukan exploit winbox dapat dilihat pada Gambar 3.



Gambar 3. Tampilan Zenmap

Tampilan Exploit IP publik mikrotik script winbox exploit menggunakan perintah python3 WinboxExploit.py dengan port 8888 dari hasil analisis port yang sudah didaptakan menggunakan zenmap, langkah selanjutnya yaitu dengan menggunkan perintah python3 WinboxExploit.py 8888 proses exploit yang dilakukan dengan alamat IP yang sudah didaptkan dengan port 8888, ternyata proses exploit berhasil dengan beberapa username dan password dari IP publik yang sudah dianalisis ternyata masih bisa diexploit dengan port 8888 sehingga dengan mudah untuk memasuki mikrotik router tersebut dapat dilihat pada Gambar 4.



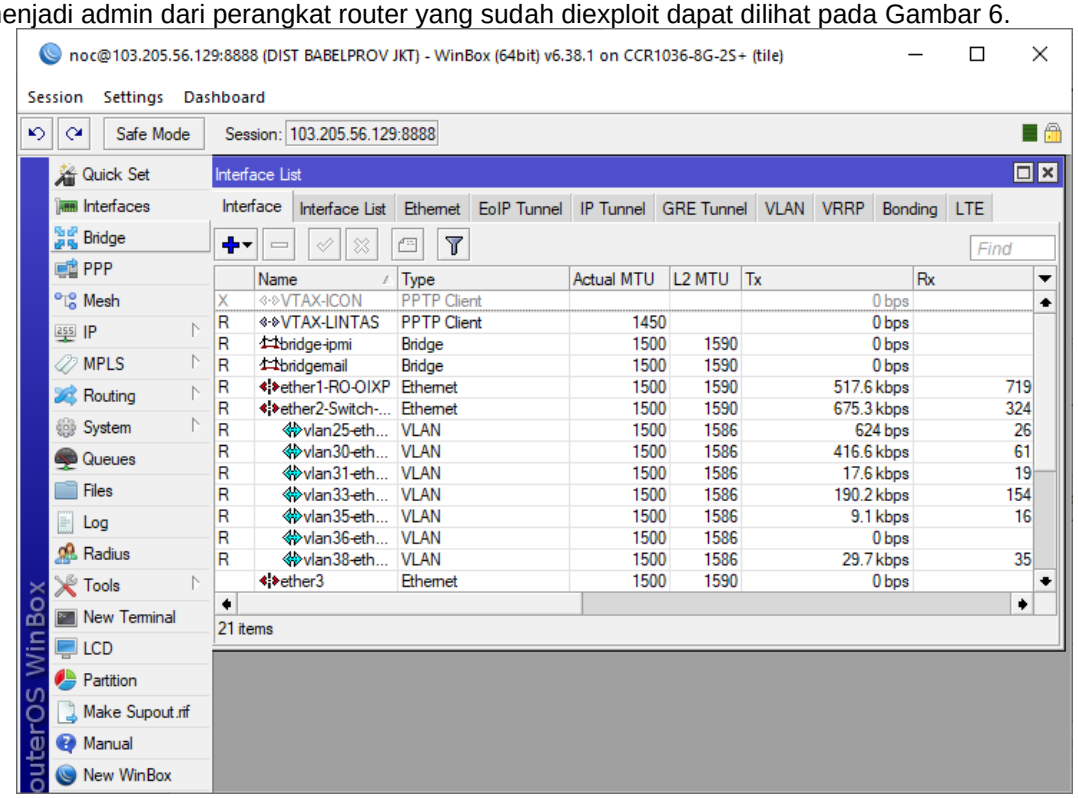
Gambar 4. Tampilan Exploit WinboxPoC Sucses

Tampilam Hasil exploit menggunakan Mroot yang sudah didapatkan secara random dari berbagai ISP sudah berhasil diexploit dengan port default 8291 dengan mikrotik v6.41.3 yang masih rentan terhadap serangan yang dapat mengambil sistem dari admin yang mengacu pada

kelemahan dari mikrotik itu sendiri terdapat celah keamanan yang dikenal dengan CVE- 2018-14847 cara kerjanya kerentanan memungkinkan alat khusus untuk menyambung ke port winbox dan meminta file database pengguna sistem, dari hasil exploit menggunakan mroot terdapat beberapa *username* dan *password* yang sudah didapatkan dari berbagai pengguna sercara random dapat dilihat pada Gambar 5.

Gambar 5. Hasil Exploit Mroot Secara Random

Tampilan hasil ujicoba IP publik mikrotik menggunakan software winbox ip publik yang sudah diexploit setelah memasukan *username* dan *password* pada winbox maka akan muncul menu halaman mikrotik routerOs ISP Pemerintah Provensi kepulauan Bangka Belitung. Dimana sudah menjadi admin dari perangkat router yang sudah diexploit dapat dilihat pada Gambar 6.



Gambar 6. Tampilan Menu halaman Winbox

KESIMPULAN

Berdasarkan hasil ujicoba analisis penelitian yang berjudul "Analisis Keamanan Jaringan Mikrotik ISP Indonesia menggunakan *Search Engine Scada Shodan* dengan Metode *Winbox Critical Vulnerability"*. Penelitian ini berhasil menyimpulkan beberapa hal terkait penelitian yang dilakukan sebagai berikut:

1. Dari hasil ujicoba menggunakan shodan terdapat beberapa IP publik masih banyak pengguna menggunakan routerOs versi 6.42-v6.28, dari hasil penelitian exploit yang telah dilakukan terdapat celah dari mikrotik routerOs versi 6.42-v6.28 kebawah terdapat celah keamanan yang dapat diexploitasi untuk mendapatkan *username* dan *password,* pada kelemahan dari mikrotik itu sendiri terdapat celah keamanan yang dikenal dengan CVE- 2018-14847 cara kerjanya kerentanan memungkinkan alat khusus seperti script winboxPoC, Mroot untuk menyambung ke port winbox dan meminta file database pengguna sistem.
2. Berdasarkan penelitian yang dilakukan hasil analisis IP publik mikrotik menggunakan Zenmap dan Termux untuk melakukan *scanning* port apa saja yang terbuka disni proses exploit akan berjalan jika tedapat satu host dan jika host 0 maka proses exploit tidak berhasil karna terdapat *firewall* maka keluar eror *timeout*.

Saran

Berdasarkan hasil rangkuman kesimpulan diatas, penulis bermaksud memberikan saran yang dapat bermanfaat untuk pihak tertentu maupun bagi penelitian yang seterusnya, yakni sebagai berikut:

1. Diharapkan penelitian selajutnya mengenai topik ini untuk pencarian IP publik menggunakan web shodan atau scada shodan sebaiknya menggunkan akun premium untuk mendapatkan IP publik tanpa adanya batasan.
2. Diharapkan penelitian selanjutnya melakukan penelusuran referensi dan informasi terbaru mengenai topik ini karena seiring perkembangan zaman dan teknologi serangan exploitasi semakin canggih yang memungkinkan terjadinya exploit yang digunakan dengan alat khusus seperti script winboxPoC, Mroot.
3. Terdapat banyak fasilitas dari perangkat router mikrotik gunakan *firewall* dengan memanpatkan *service* diwinbox, batasi akses mikrotik menggunakan alamat IP yang sudah ditentukan agar terhindar dari serangan, agar meningkatkan keamanan jaringan komputer dengan baik serta sesuai dengan kebutuhan instansi atau perusahaan.

DAFTAR PUSTAKA

Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, 35-38.

Autotekno. (2018, Agustus 31). *MikroTik di Indonesia Diserang Besar-Besaran CryptoJacking*. Retrieved from https://autotekno.sindonews.com/berita/1334444/133/mikrotik-di-indonesia-diserang-besar-besaran-cryptojacking: https://autotekno.sindonews.com

Bssn. (2018, October 16). *Himbauan Terkait Kerentanan CVE-2018-14847*. Retrieved from https://bssn.go.id/himbauan-terkait-kerentanan-cve-2018-14847/: https://bssn.go.id

Chandra, S., Hutauruk, Yulianto, Y., & Satrya, &. (2016). Malware Analysis Pada Windows Operating System Untuk Mendeteksi Trojan Malware Analysis on Windows Operating System To Detect Trojan. *e-Proceeding of Engineering*, 3590–3595.

Khayudi, M. A. (2019). Analisis dan Perancangan Keamanan Akses Router Mikrotik dari Serangan Exploit. *DIGITAL REPOSITORY Universitas Internasional Batam*, 1-81.

Prayudi, Y., & Putro, D. H. (2018). simulasi untuk peningkatan keamanan data pada metarouter yang sudah tereksploitasi. *Universitas Islam Indonesia*.

Santoso, J. D. (2019). Uji Kerentanan Keamanan Server Menggunakan Scada Shodan. *TEKNOKOM* , vol 2 -no 2.

Shaifullah, S. M. (2018). desain firewall terhadap serangan ddos pada router mikrotik. *Universitas Mercu Buana Yogyakarta*.

Shodan. (2009). *The search engine for the Internet of Things*. Retrieved from https://www.shodan.io/search?query=mikrotik+country%3A%22ID%22: https://www.shodan.io