Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 6, No. 11, November 2021

PENERAPAN DIGITAL SECURITY UNTUK ANALISIS SERANGAN KEAMANAN JARINGAN VOIP DENGAN METODE PENETRATION TESTING

Ramadhan Dwi Putra, Arip Solehudin, Nono Heryana
Universitas Singaperbangsa Karawang (UNSIKA) Jawa Barat, Indonesia
Email: ramadhan.dwi17173@student.unsika.ac.id, arip.solehudin@unsika.ac.id, nono@unsika.ac.id

Abstrak

Tujuan penelitian ini adalah untuk meningkatkan dan mengembangkan keamanan VoIP menggunakan metode *Penetration Testing*. Metode *Penetration Testing* merupakan metode untuk menguji keamanan sebuah sistem untuk dicari kelemahan dan kerentanannya. Penelitian ini akan dilakukan di GM Purinet Kosambi. Hasil penelitian ini menunjukkan bahwa keamanan sistem memang perlu ditingkatkan dari sudut manapun. Berdasarkan hasil penelitian *Penetration Tetsing* berhasil untuk melakukan evaluasi keamanan suatu sistem.

Kata Kunci: VoIP; penetration testing

Abstract

The purpose of this research is to improve and develop VoIP security using the Penetration Testing method. Penetration Testing method is a method for testing the security of a system that is looking for weaknesses and vulnerabilities. This research will be conducted at GM Purinet Kosambi. The results of this study indicate that system security does need to be improved from any angle. Based on the research results, the Penetration Testing was successful in evaluating the system assessment.

Keywords: *VoIP; penetration testing*

Received: 2021-10-20; Accepted: 2021-11-05; Published: 2021-11-20

Pendahuluan

VoIP menjadi salah satu media komunikasi yang banyak digunakan di kalangan semua pengguna seperti sekolah, universitas maupun perusahaan. Dengan VoIP kita lebih mudah untuk berkomunikasi melalui suara maupun gambar. Menurut (Hsieh & Leu, 2018) teknologi ini banyak digunakan karena sangat efektif dalam penanganan komunikasi, dengan memanfaatkan jaringan lokal tanpa harus mengeluarkan biaya untuk berkomunikasi dalam satu lingkup lingkungan. Didalam teknologi VoIP terdapat komponen keamanan yang paling diperhatikan yaitu data suara dan gambar,

How to cite: Putra. R.D., Arip Solehudin & Nono Heryana (2021) Penerapan Digital Security Untuk Analisis Serangan Keamanan Jaringan Voip Dengan Metode Penetration Testing. *Syntax Literate: Jurnal Ilmiah Indonesia*, *6*(11). http://dx.doi.org/10.36418/ Syntax-Literate.v6i11.3556

E-ISSN: 2548-1398
Published by: Ridwan Institute

(Nurnaningsih & Permana, 2018) menyampaikan bahwa untuk menghindari adanya penyadapan terhadap kedua komponen tersebut maka dari setiap interaksi pada teknologi VoIP menggunakan enkripsi data pada protokol SIP (*Session Initiation Protocol*) dan RTP (*Real Time Protocol*) yang menggunakan metode kriptografi seperti AES (*Advanced Encryption Standard*), *Twofish* dan macam-macam algoritma lainnya sehingga pesan yang dikirim ataupun diterima hanya dapat diketahui oleh pihak yang bersangkutan saja. Teknologi ini pun akhirnya menjadi sorotan bagi seorang *cyber* karena pada teknologi VoIP ini di dalamnya terjadi sebuah transaksi data seperti audio dan video. *Digital Security* atau disebut keamanan digital merupakan solusi untuk melindungi identitas digital berdasarkan pada perangkat pribadi, *platform* layanan dan perangkat lunak. Hal ini perlu diterapkan pada masing-masing digital yang tersambung pada teknologi VoIP dan jika tidak, maka data ini yang nantinya dapat digunakan oleh seorang *cyber* yang tidak bertanggung jawab dengan dan dimanfaatkan untuk keuntungan sendiri.

GM Purinet Kosambi merupakan sebuah usaha dibidang jaringan RT/RW yang telah beroperasi selama 2,5 tahun, memiliki surat izin usaha dan juga memiliki teknologi VoIP didalam jaringannya dengan *bandwidth* yang dimiliki sebesar 100Mbps. GM Purinet Kosambi menggunakan teknologi VoIP sebagai komunikasi kepada pihak dengan menggunakan koneksi jaringan lokal untuk memberikan informasi apabila *user* tidak dapat mengakses internet. Umumnya VoIP *service* membutuhkan setidaknya 100Kbps *upload* dan *download* untuk 1 *user* panggilan namun kecepatan yang direkomendasikan sebesar 3 Mbps agar mendapatkan kualitas panggilan yang lebih baik, tetapi jaringan GM Purinet Kosambi ini hanya sebatas mem-*forward network* yang berbeda menjadi saling terhubung tanpa adanya keamanan *filtering* seperti mengaktifkan *firewall* jaringan, menutup *port* jaringan tertentu dan lain sebagainnya, sehingga berpotensi adanya serangan pada jaringan. Hal ini dapat mengakibatkan terjadinya pencurian data berupa gambar, video dan suara kepada seluruh *client* yang terhubung pada jaringan GM Purinet.

Keamanan jaringan VoIP sangat penting dalam sebuah arsitektur jaringan karena VoIP merupakan jembatan atau gerbang bagi seorang *cyber* untuk melakukan tindak kejahatan. Dari VoIP banyak celah yang dapat dilalui, resiko yang didapat bisa merusak, melemahkan bahkan tercurinya data. Mengutip (Kolhar, 2017) tanpa adanya keamanan pada jaringan VoIP resiko kerugian akan sangat besar karena harus mencari celah mana yang dilalui oleh seorang *cyber*. Terdapat macam-macam keamanan utama pada teknologi VoIP ini seperti VoIP *call private network*, *Firewall and packetized voice* dan VoIP *lockdown* yang bertujuan untuk melindungi perangkat yang tersambung pada jaringan VoIP dari *sniffing voice*, *delayed traffic voice* bahkan penyalahgunaan dan pencurian data. Baru-baru ini VoIP tidak hanya menyerang melalui protokol TCP/IP saja melainkan melalui protokol SIP dan RTP yang biasa digunakan untuk enkripsi data antar pengguna VoIP (Sadiwala, 2018). Masalah umum yang muncul pada keamanan VoIP yaitu *delayed traffic voice* yang disebabkan oleh serangan DDoS pada, kemudian munculnya *caller id spoofing* dengan tujuan untuk mendapatkan informasi yang

diinginkan. Maka dari itu perlu dibangun keamanan jaringan dan untuk melakukannya harus dilakukan tes uji coba serangan pada jaringan VoIP untuk mengetahui celah dan meningkatkan keamanan terhadap celah tersebut. Dengan adanya keamanan pada jaringan VoIP seorang *cyber* tidak akan mudah masuk ke dalam sistem karena celah yang dilalui tertutup dan tidak mendapatkan hak akses izin untuk masuk ke dalam sistem.

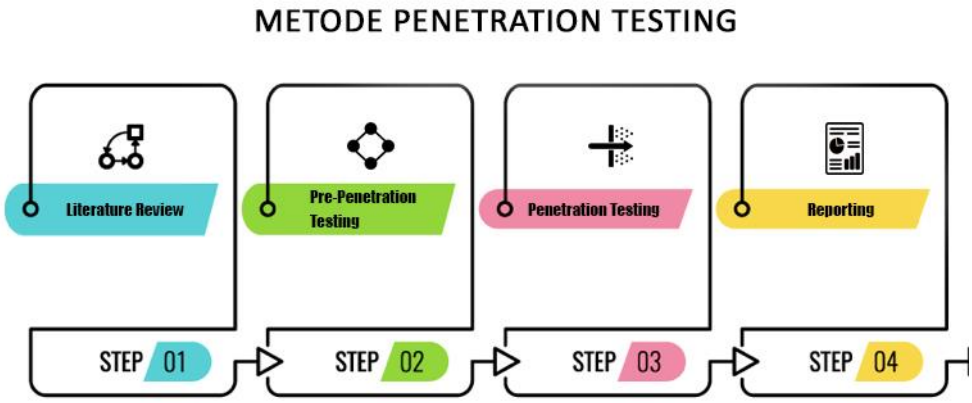
Berdasarkan penelitian sebelumnya dari (Ochang & Irving, 2017) dalam penelitian yang berjudul "*Security Analysis of VoIP Networks Through Penetration Testing*", menyatakan bahwa metode *Penetration Testing* merupakan metode yang biasa digunakan dalam mengungkapkan permasalahan jaringan administrator yang tidak teridentifikasi, metode ini digunakan sebagai perencanaan dalam mengumpulkan informasi dengan cara menargetkan serangan terhadap sistem itu sendiri, serangan yang diujicobakan adalah serangan yang biasa digunakan atau serangan yang dapat dilakukan terhadap arsitektur sistemnya dan hasil dari percobaannya digunakan untuk menutupi kemungkinan serangan-serangan yang dapat merusak sistem. Hasil yang didapatkan pada penelitian ini menunjukan 2 *user* PBX yang menggunakan protokol SIP berhasil disadap melalui *port* jaringan yang tidak ditutup yaitu *port* 5060 menggunakan sip*vicious* dan nmap dan saat itu juga *user* PBX yang berada dalam kondisi *offline* digunakan untuk melakukan *Spoofing Caller ID*.

Penelitian selanjutnya yang dilakukan Deni Satria dan rekannya pada penelitian yang berjudul "*Network Security Assesment Using Internal Network Penetration Testing Methodology*" mendapatkan hasil dari implementasi metode *penetration testing* bahwa dalam melakukan *autentication attack*, kerentanan pada setiap perangkat mencapai 20% - 80%. 60% pada perangkat yang diuji cobakan dapat diretas menggunakan XSS *attack* untuk merubah *default username* dan *password* sebagai proses masuk kedalam sistem (Satria et al., 2018).

Metode Penelitian

A. Alur Penelitian

Metode penelitian yang digunakan adalah *Penetration Testing*, metode penelitian yang dilakukan secara kualitatif yaitu dengan terjun dan masuk ke dalam lapangan agar dapat melihat serta merasakan fakta apa yang sebenarnya terjadi. Tahapan penelitian yang akan dilakukan mengikuti tahapan-tahapan dari metode *Penetration Testing* yaitu *Literature Review*, *Pre Penetration Testing*, *Penetration Testing*, *Reporting*.



Gambar 1
Alur Penelitian *Penetration Testing*

B. Literature Review

Pada tahap ini peneliti melakukan pemahaman mengenai keamanan VoIP yang akan diterapkan pada jaringan GM Purinet Kosambi dan didapatkan hasil bahwa terdapat 3 buah komponen keamanan yang diterapkan dalam VoIP yaitu:

1. VoIP *Call Private Network*

VoIP merupakan teknologi yang menggunakan data *packet* serupa halnya dengan teknologi yang digunakan oleh jaringan LAN dan WAN. Maka dari itu perlu adanya *call privacy* dengan solusi me-*route voice traffic over* dengan *private network*. Hal ini untuk menghindari penyadapan *voice traffic* melalui jaringan itu sendiri yang bersifat publik.

2. Firewall dan *Packetized Voice*

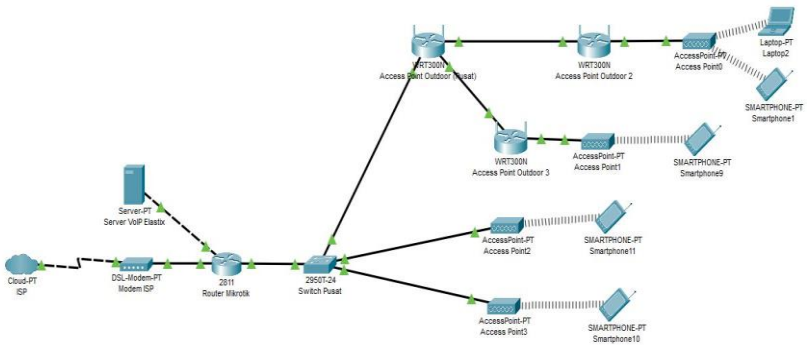
VoIP menggunakan protokol jaringan TCP sebagai jalur komunikasi menuju ke *end-user* dan bersifat *real-time* dengan menggunakan protokol RTP (*Real Time Protocol*). Lalu VoIP menggunakan protokol SIP untuk membangun jalur komunikasi yang dikhusukan untuk *voice over*. Dengan adanya sebuah *firewall*, sebuah paket akan ditangkap berdasarkan kebutuhan dari protokol yang digunakan.

3. VoIP *Lockdown*

Didalam teknologi VoIP, *server* diibaratkan seperti jantung dalam proses komunikasi. Perlu adanya pemeliharaan untuk mencari kekurangan baik dari segi *software* seperti sistem operasi, aplikasi *softphone* dan dari segi *hardware* seperti infrastruktur topologi jaringan dan perangkat jaringan yang digunakan.

C. *Pre Penetration Testing*

Pada tahap ini dilakukan pembuatan topologi sistem jaringan VoIP sebagai gambaran infrastruktur yang sesuai dengan jaringan GM Purinet dengan tujuan mengetahui alur serangan, akses jaringan lokal dan jaringan luar yang dapat dilakukan untuk penyerangan dengan metode *penetration testing*.



Gambar 2
Topologi Jaringan

Topologi diatas menggambarkan alur serangan yang akan dilakukan dimana topologi jaringan didapatkan dari gambaran yang sesuai dengan topologi jaringan GM PURINET KOSAMBI. Dilihat dari gambar topologi alur serangan terdapat sebuah lingkaran merah menandakan uji penetrasi dilakukan melalui jaringan *client* dimana *attacker* berperan sebagai *client* pada jaringan yang terhubung langsung dengan jaringan *server* sebagai komunikasi VoIP, kemudian melakukan *penetration testing* terhadap sistem VoIP untuk mengetahui kerentanannya.

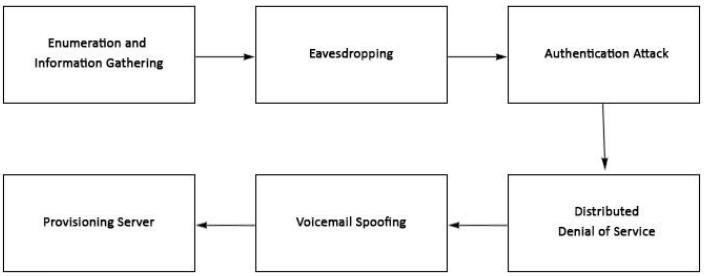
Pada tahap ini juga peneliti melakukan observasi dan wawancara kepada administrator jaringan dan juga *client* yang menggunakan GM Purinet Kosambi untuk mengetahui *software* dan *hardware* apa yang digunakan dalam proses penerapan teknologi VoIP dan didapatkan penggunaan yang terurai pada tabel 1:

Tabel 1
Software dan Hardware

Hardware	1. Mikrotik Routerboard HEX Series 2. Hub TPLink TL SF1008D WK01 3. Converter Fiber Optic NETLINK HTB-3100 AB 4. Access Point TPLINK TLWR840N 300MBps 5. Mikrotik HAP-Lite 6. Tplink CPE 220 Outdoor
Software	1. Sistem Operasi Elastix VoIP 2. WinBox 3. Zoipper

D. *Penetration Testing*

Tahap ini dilakukan uji penetrasi terhadap *server* VoIP melalui jaringan *client* yang terhubung langsung dengan jaringan GM Purinet dengan menggunakan sistem operasi kali linux, ditahap penetrasi ini dibagi menjadi 6 bagian yaitu tahap awal mengumpulkan informasi, melakukan penyadapan komunikasi, serangan autentikasi, membanjiri paket ke *server*, melakukan penyamaran dan mengidentifikasi tata letak *server*.



Gambar 3
Tahapan Penetrasi

Pada gambar 3 tahapan penetrasi dilakukan secara bertahap guna untuk mengetahui kelemahan VoIP baik dari segi *software* seperti sistem operasi *server* dan aplikasi yang digunakan untuk berkomunikasi maupun *hardware* seperti perangkat jaringan, perangkat keras *server* yang digunakan.

E. *Reporting*

Pada tahap ini memberikan hasil eksploitasi dan laporan terkait dampak uji coba serangan terhadap sistem yang telah dilakukan untuk memberikan kesimpulan dan juga keputusan dalam mengamankan sistem.

Hasil dan Pembahasan

A. Hasil Penelitian

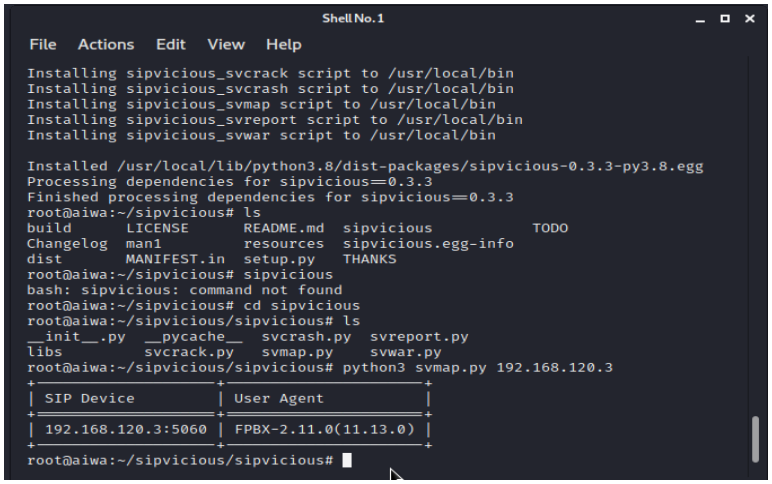
Hasil penelitian yang sedang dilakukan adalah bagaimana cara untuk mengetahui jenis-jenis dan bentuk serangan VoIP guna melindungi sistem VoIP pada jaringan GM Purinet Kosambi dari ancaman kerusakan sistem maupun kerugian tercurinya data pengguna jaringan. Hasil yang didapatkan berupa analisis dengan bantuan menggunakan metode *Penetration Testing*.

1. *Enumeration and Information Gathering*

Pada tahap ini dilakukan sebuah pencacahan untuk mengetahui informasi mengenasi keseluruhan yang ada pada sistem, seperti *server* dengan sistem operasi jenis apa yang digunakan dan ada berapa jenis ekstensi yang digunakan.

2. *Scanning*

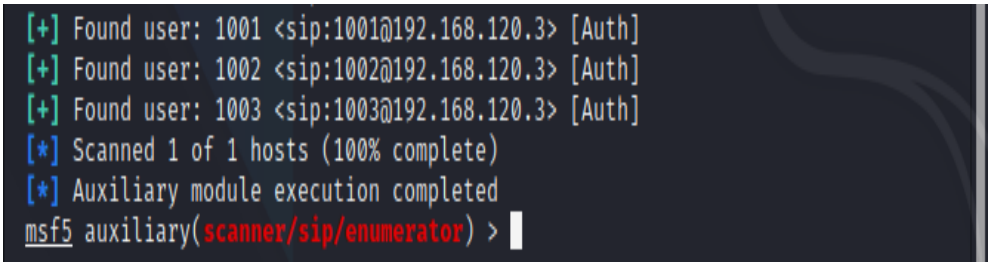
Untuk mengetahui sistem operasi yang digunakan pada sistem jaringan VoIP perlu dilakukan *scanning* terlebih dahulu. Untuk melakukan *scanning tools* yang digunakan adalah *tools* SIP*Vicious*. Tools ini dapat melakukan *scanning* sistem berdasarkan ip *address* VoIP.



Gambar 4
Hasil *scanning* sv*map*.py

Pada gambar 4 menunjukkan hasil *scanning* yang telah dilakukan oleh *tools* sv*map*.py bahwa *server* VoIP pada sistem jaringan dengan IP *server* 192.168.120.3 *port* 5060 menggunakan sistem operasi Elastix (*Free*PBX).

Kemudian untuk mengetahui berapa jumlah *extension* yang menggunakan protokol SIP pada digunakan *tools metasploit-framework*.

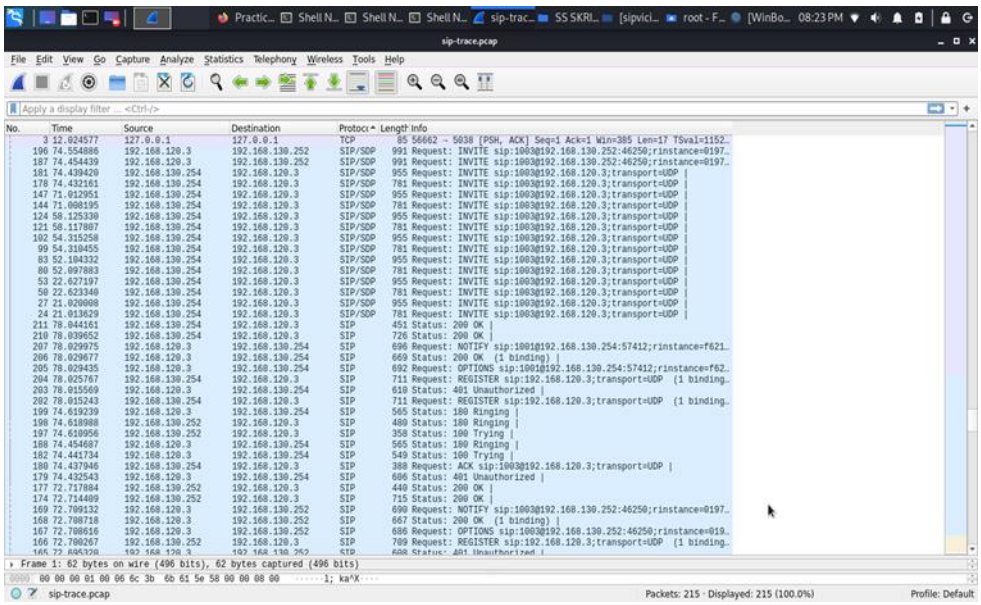


Gambar 5
Hasil *scanning extension*

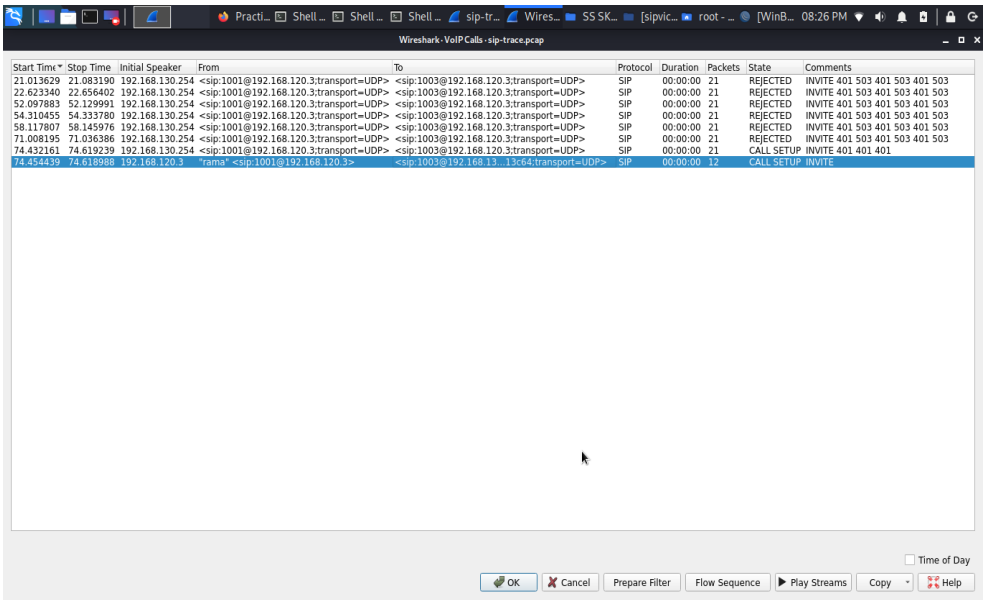
Pada gambar 5 didapatkan hasil *scanning* yang dilakukan menggunakan *metasploit-framework*. Hasil yang didapat adalah *extension* yang digunakan didalan VoIP berjumlah 3 yaitu *user* dengan *extension* 1001,1002 dan 1003.

3. *Eavesdropping*

Tahap in dilakukan untuk menguping pembicaraan panggilan dengan menangkap paket dari protokol SIP dan RTP dari *smartphone* ke. Proses yang akan dilakukan yaitu dengan menggunakan metode MITM (*Man in The Middle*) untuk melakukan penyegatan terhadap lalu lintas pengguna yang terhubung pada VoIP.



Gambar 6
Merekam paket dengan *wireshark*



Gambar 7
VoIP *calls detail*

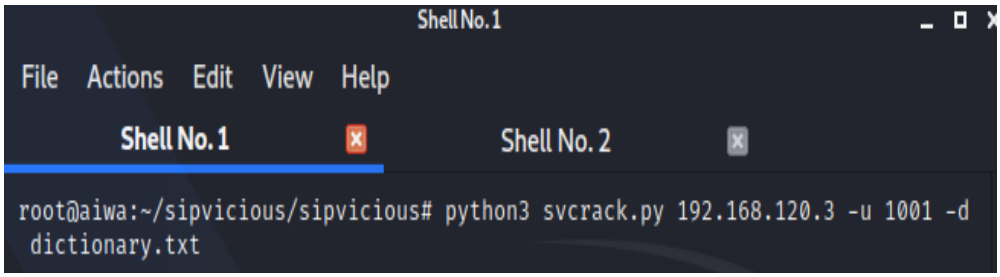
Pada gambar 6 didapatkan paket-paket dengan protokol SIP, hal ini menandakan bahwa selama proses perekaman terjadi proses komunikasi pada . Kemudian hasil paket yang didapatkan melalui proses perekaman dimana *user* "rama" dengan extension 1001 diketahui telah melakukan *call invite* terhadap *user* dengan *extension* 1002 yang dijelaskan pada gambar 7.

4. Authentication Attack

Pada tahap ini dilakukan serangan autentikasi terhadap guna untuk mengetahui informasi mengenai *username* dan *password* dari masing-masing

extension, untuk melakukannya dibutuhkan salah satu *tools* dari SIP*Vicious* yaitu sv*crack*.py dan *dictionary*.txt.

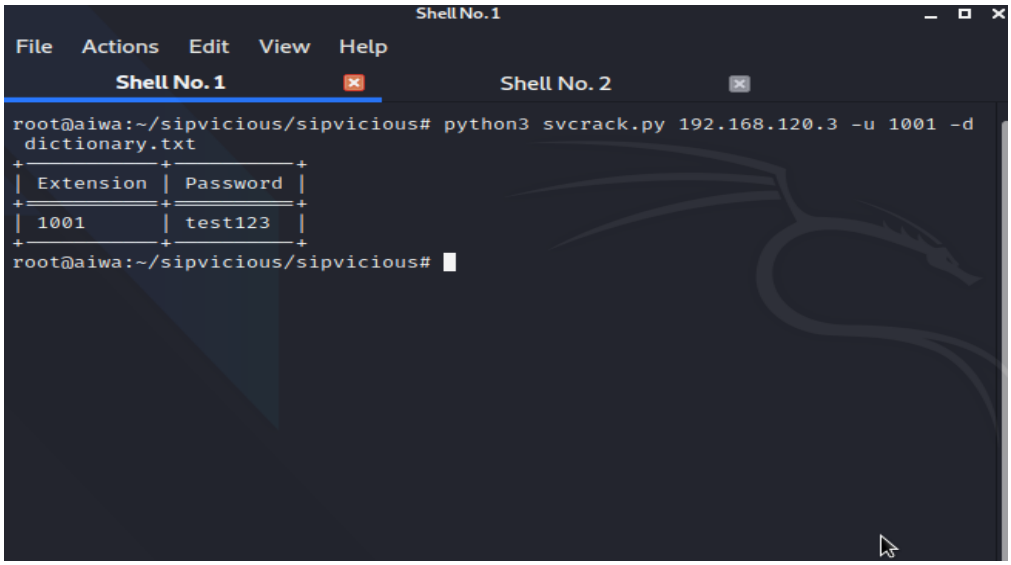
Dictionary.txt merupakan sekumpulan *wordlist* yang terdiri dari ratusan ribu kata, gunanya untuk mencocokkan sebuah kata yang serupa dengan apa yang ingin di-*compare* sesuai dengan kebutuhan.



Gambar 8
***Authentication Attack* dengan sv*crack*.py**

Pada gambar 8 menjelaskan *command* dimana *tools* sv*crack*.py akan menscanning *password* dari *user* SIP 1001 dengan mencocokkan *file* dari *dictionary*.txt. Proses ini membutuhkan waktu untuk mencocokkan antara *file wordlist* dengan sistem.

Kemudian pada gambar 9 didapatkan hasil dari *scanning tools* sv*crack* bahwa *password* dengan *user* 1001 adalah “test123”.

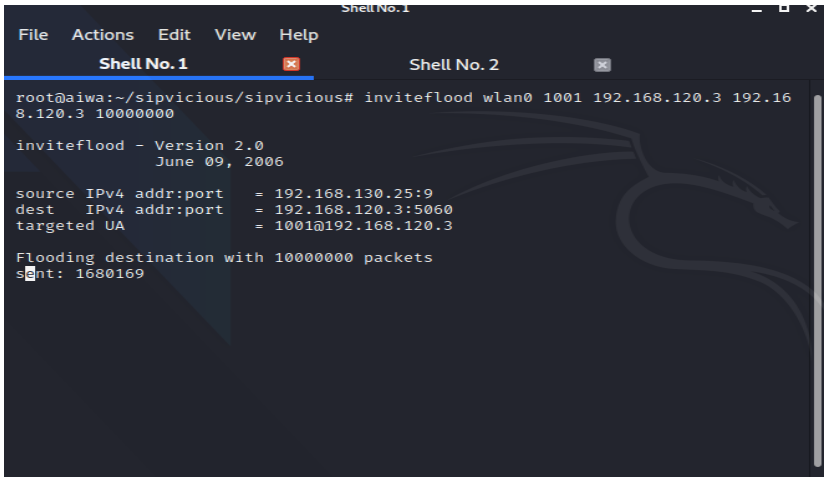


Gambar 9
Hasil *Authentication Attack*

5. *Denial of Service Attack*

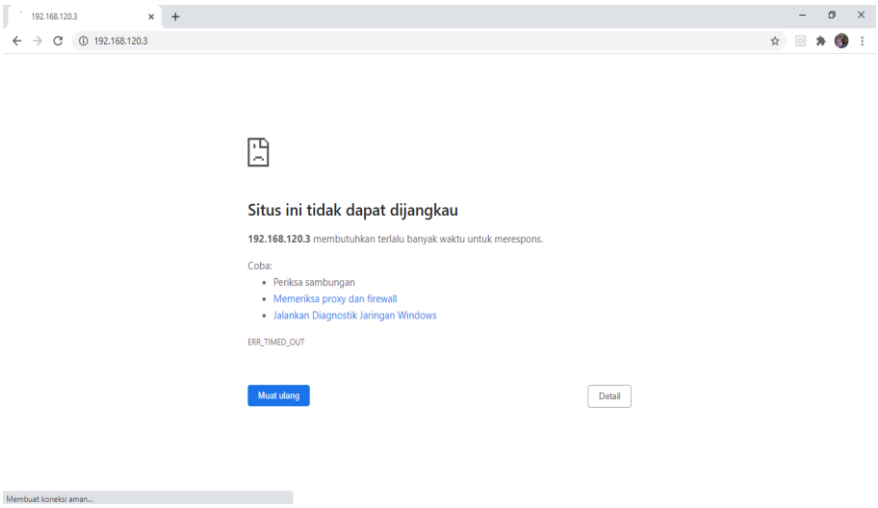
Pada tahap ini dilakukan untuk membanjiri lalu lintas paket jaringan terhadap agar mengalami gangguan dan tidak dapat merespon permintaan *user*

SIP dalam melakukan panggilan, dibutuhkan *tools inviteflood* untuk melakukan serangan ini.



Gambar 10
DDoS *Attack* dengan *Inviteflood*

Gambar 11
Uji coba panggilan

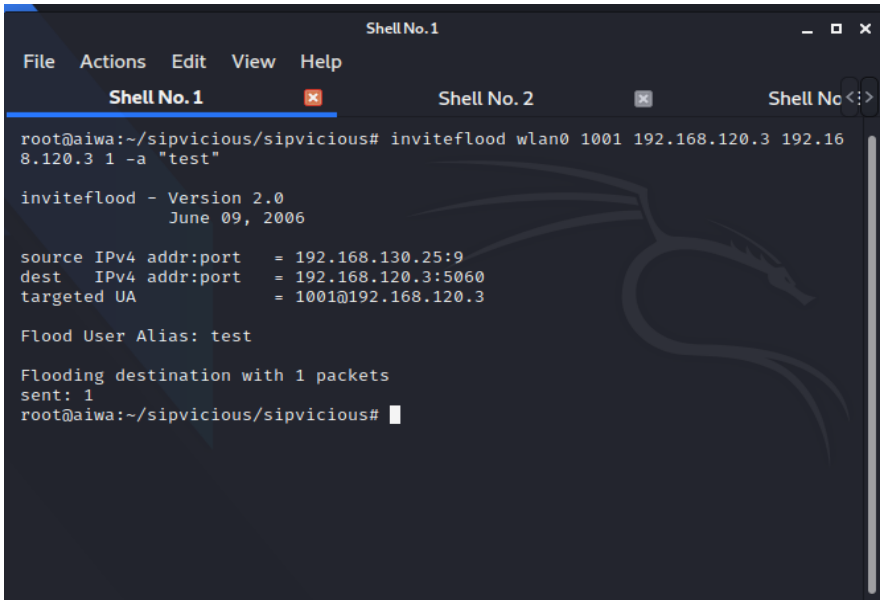


Gambar 12
***Server* VoIP tidak dapat diakses**

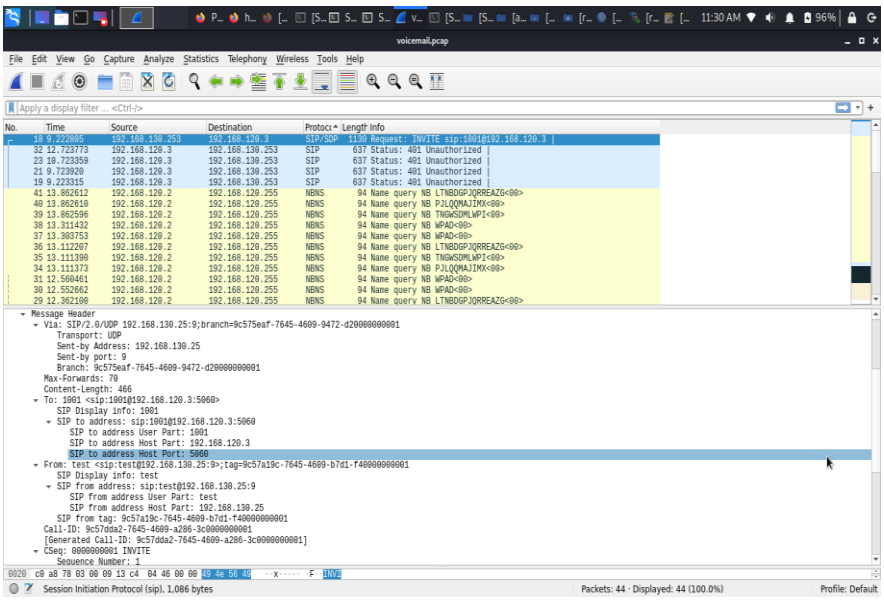
Selama proses penyerangan DDos telihat pada gambar 11 dimana *user* SIP 1002 melakukan uji coba panggilan terhadap *user* SIP 1001, tetapi tidak ada respon panggilan masuk pada *user* SIP 1001. Hal ini dikarenakan sedang dibanjiri paket data sebesar 1 juta paket sehingga tidak dapat merespon permintaan client. Bahkan selama proses penyerangan, voip berbasis *web base* untuk memanajemen sistem voip sama sekali tidak dapat diakses, hal ini dibuktikan pada gambar 12.

6. *Voicemail Spoofing*

Pada tahap ini dilakukan penyamaran sebagai *user* SIP yang terdaftar terhadap, tujuannya untuk mendapatkan data yang dibutuhkan seorang penyerang terhadap *user client* yang lainnya.



Gambar 13
Voicemail Spoofing* dengan *Inviteflood



Gambar 14
Pembuktian *spoofing mail*

Pada gambar 13 penyamaran dilakukan untuk mengirim sebuah *message* "*test*" ke *user* SIP 1001, *user* SIP 1001 akan menerima *mail* dari *user* "*test*" seolah itu merupakan *user* yang dapat dipercaya karena *user* tersebut terdaftar didalam VoIP. Hasil tersebut dapat dilihat pada tanda warna merah. Kemudian dibuktikan melalui *capture wireshark* pada gambar 14, selama perekaman atas aktivias yang dilakukan pada VoIP didapatkan hasil *testing* yang dilakukan oleh *user* "*test*" ke *user* SIP "1001".

7. *Provisioning*

Setelah melakukan wawancara, VoIP pada GM PURINET menggunakan sistem *virtual machine*. Hal ini dapat dimanfaatkan dalam hal pencurian data dikarenakan *virtual machine* yang digunakan 1 jaringan dengan *host* asli dari perangkat yang digunakan sekaligus mendapatkan 2 buah induk *file*.

B. Pembahasan

Hasil penelitian yang didapatkan dari metode Penetration Testing pada jaringan VoIP GM Purinet Kosambi dapat diterapkan sehingga menghasilkan informasi dan reporting mengenai kelemahan dan kerentanan pada sistem VoIP, yaitu:

Tabel 2
Pembahasan

Celah yang didapat	Dampak	Solusi
Informasi SIP Device *Server*	Penyerang mendapatkan informasi detail mengenai sistem operasi yang digunakan pada *server*	Menutup informasi port IP *server* atau menyembunyikan informasi OS name
Informasi SIP Account	Penyerang mendapatkan informasi mengenai SIP account yang ada pada *server*	Menggunakan ID account dengan rentang angka 10 atau 11 digit
Mendapatkan paket palsu yang mengatas namakan ip client	User SIP yang terdaftar pada *server* tidak dapat melakukan request dikarenakan requestnya telah digunakan oleh si penyerang	Memfilter request packet pada *server* berdasarkan protokol yang digunakan agar diketahui jelas asal-usul keberadaan paket
Mendapatkan aktivitas paket jaringan dengan protokol SIP	Penyerang mengetahui aktivitas yang terjadi pada *server* VoIP	Protokol SIP harus dienkripsi menggunakan enkripsi TLS agar informasi tidak dapat dibaca oleh penyerang
Mendapatkan User ID dan Password SIP Client melalui IP *Server*	Penyerang dapat menggunakan User SIP demi keuntungan pribadi	Uuser SIP menggunakan kombinasi abjad, nomor, special character agar password tidak mudah diketahui
Mengirimkan 100000 request paket ke *server*	User dan admin tidak dapat melakukan akses pada *server* VoIP	Menggunakan identifikasi menggunakan syn flood dan cloudfare agar dapat memfilter paket-paket yang sesuai
Mengirimkan message palsu ke target user SIP yang dituju	Client beranggapan bahwa pesan yang diterima berasal dari user yang dimaksud	User SIP menggunakan SIP alias agar username pada setiak akun tidak dapat digunakan sembarang oleh

	tetapi pesan tersebut berasal dari penyerang	orang lain
Memastikan message palsu terkirim	-	-
Server menggunakan virtual machine yang menyatu dengan host komputer yang digunakan	Penyerang dapat melakukan pencurian data pada kedua file induk melalui IP *server*	*Server* menggunakan mesin yang dikhususkan untuk kegiatan VoIP dan menggunakan fitur SIP trunks agar beberapa informasi akun SIP terselamatkan

Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa GM PURINET KOSAMBI memiliki sistem jaringan VoIP untuk para *client* melakukan pelaporan mengenai koneksi internetnya tetapi kurangnya manajemen keamanan pada teknologi yang digunakan. Sehingga dengan melakukan uji coba penetrasi dengan metode *Penetration Testing* menjadi solusi agar mengetahui titik lemah sistem VoIP pada jaringan. Dengan mengetahui kerentanan pada sistem VoIP akan membantu admin jaringan melakukan identifikasi lebih awal dalam melakukan peningkatan keamanan sistem.

BIBLIOGRAFI

Alfiasyahri, S., & Simanjuntak, P. (2020). Jurnal Comasie. *Aplikasi Pembelajaran Bahasa Latin Tumbuh-Tumbuhan Berbasis Android*, *3*(3), 21–30. Google Scholar

Bhandari, S. (2016). *VOIP : Security issues , Security Mechanism and Inherit*. *6913*(June), 132–139. Google Scholar

Carvajal L, Chen L, Varol C, Rawat D. Detecting unprotected SIP-based Voice over IP traffic. In2016 4th International Symposium on Digital Forensic and Security (ISDFS) 2016 Apr 25 (pp. 44-48). IEEE. Google Scholar

Gede, S. S. A. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati*, *8*(2), 113–124. Google Scholar

Hanipah, R. (2020). *WIRESHARK*. *4*(1), 11–23. Google Scholar

Hsieh, W. Bin, & Leu, J. S. (2018). Implementing a secure VoIP communication over SIP-based networks. *Wireless Networks*, *24*(8), 2915–2926. https://doi.org/10.1007/s11276-017-1512-3 Google Scholar

Ilmu, J., Fakultas, K., & Universitas, M. (n.d.). *Penggunaan Metode Kriptografi Pada Voice*. 473–479.

Isnanta, A. W., & Kurniawan, M. T. (2017). Perancangan Jaringan Multiprotocol Label Switching Menggunakan metode NDLC Untuk Layanan VOIP DAN Streaming Video Universitas Telkom. *Proceeding of Engineering*, *4*(2), 3049–3056. Google Scholar

Kolhar, M. (2017). Performance evaluation of framework of VoIP / SIP *server* under virtualization environment along with the most common security threats. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-017-2886-y Google Scholar

Mardiah, L. W., Sanjoyo, D. D., Elektro, F. T., & Telkom, U. (2019). *Comparative Analysis of Qos Between Rtp and Srtp At Call Center*. *6*(2), 3343–3350. https://libraryeproceeding.telkomuniversity.ac.id/index.php/engineering/article/viewFile/9635/9504

Nurnaningsih, D., & Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). *Jurnal Teknik Informatika*, *11*(2), 177–186. https://doi.org/10.15408/jti.v11i2.7811 Google Scholar

Ochang, P. A., & Irving, P. (2017). Security analysis of VoIP networks through penetration testing. *Communications in Computer and Information Science*, *756*, 601–610. https://doi.org/10.1007/978-3-319-67642-5_50 Google Scholar

Prasetyo, J. A., & Suardinata, I. W. (2020). Comparison of Voice over Internet Protocol (VoIP) Performances in Various Network Topologies. *Buletin Pos Dan Telekomunikasi*, *18*(1), 65. https://doi.org/10.17933/bpostel.2020.180105 Google Scholar

Putra, D. P., Ahdan, S., Studi, P., Informasi, T., Indonesia, U. T., Informatika, P. S., & Indonesia, U. T. (n.d.). *Analisis Keamanan Voice Over Internet Protocol (VOIP) Menggunakan PPTP dan ZRTP 1,3*. *x*.

Rusdi, M. I., & Prasti, D. (2019). *Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux*. 260–269. Google Scholar

Sadiwala, R. (2018). *Analysis of Security Threats of VoIP Systems*. *2581*, 34–46. Google Scholar

Santoso, K. (2016). Konfigurasi dan Analisis Performansi Routing OSPF pada Jaringan LAN dengan Simulator Cisco Packet Tracer Versi 6.2. *Jurnal Kajian Teknik Elektro*, *1*(1), 67–78. Google Scholar

Satria, D., Alanda, A., Erianda, A., & Prayama, D. (2018). Network security assessment using internal network penetration testing methodology. *International Journal on Informatics Visualization*, *2*(4–2), 360–365. https://doi.org/10.30630/joiv.2.4-2.190 Google Scholar