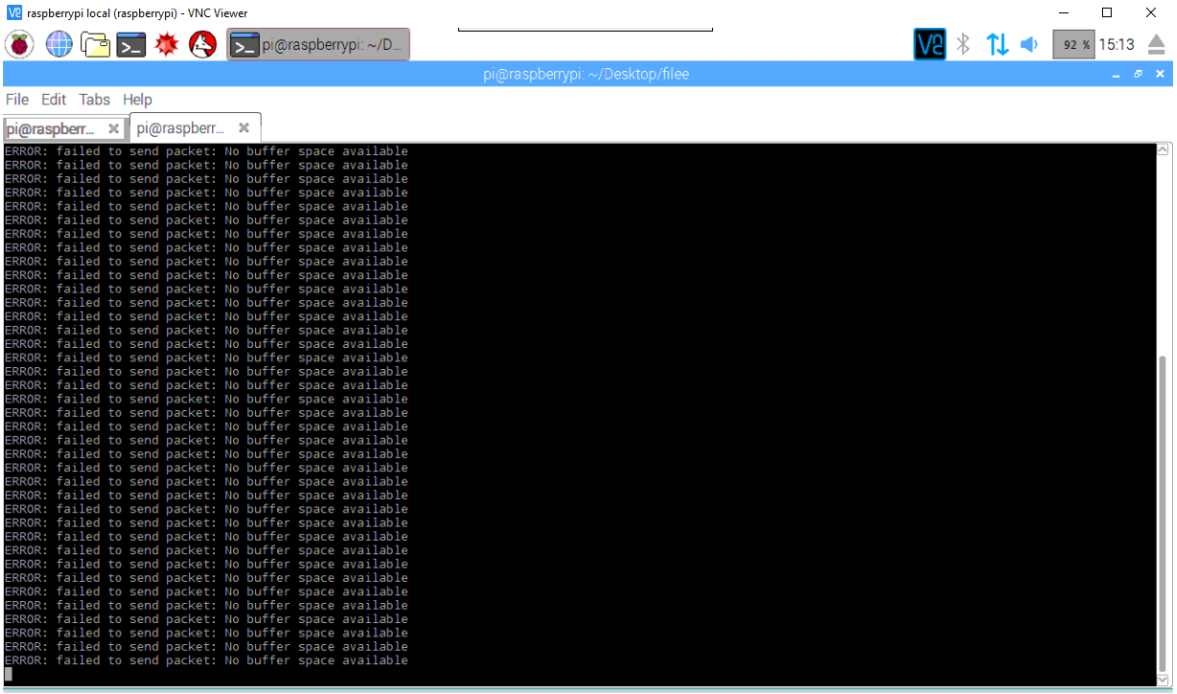
Lalu kondisi pada raspberry pi sebagai target dari serangan DOS dapat dilihat pada gambar 9. Terlihat pada terminal raspberry pi terdapat tulisan “ERROR: failed to send packet: no buffer space available” yang menandakan server (terminal) tidak dapat melakukan servis dikarenakan tidak ada ‘ruang kosong’ untuk memproses program.



Gambar 9 Keadaan Target yang Diserang oleh DOS

Pada gambar 9 dibagian pojok kanan atas terlihat indikator pemakaian CPU menunjukan angka 92%, padahal pada raspberry pi hanya menjalankan sebuah terminal saja yang tidak memerlukan banyak pemakaian CPU. Hal tersebut menunjukan bahwa serangan DOS yang dilancarkan berhasil mengenai target.

5. Kesimpulan

Pada prototipe KES yang dibangun reaksi kunci ketika dipicu memiliki rata-rata waktu 1-4 detik. Dikarenakan adanya faktor yang berpengaruh terhadap waktu reaksi kunci, yaitu *device* itu sendiri. Kemudian jarak terjauh untuk *smartphone* dan router dapat terhubung adalah sekitar 13 meter. Angka tersebut didapatkan karena kemampuan router untuk memancarkan sinyal dan kemampuan *smartphone* untuk menerima sinyal itu sendiri. Untuk serangan DOS, ketika dilancarkan akan memakan sumber dari CPU dikarenakan tool yang dipakai memuat suatu eksekusi. Kuat atau lemahnya serangan DOS dipengaruhi oleh seberapa bagus spesifikasi laptop yang digunakan. Misalnya laptop yang memiliki CPU dengan *core* banyak akan lebih kuat dibandingkan dengan CPU yang memiliki *core* lebih sedikit. Karena dengan *core* yang banyak, jumlah eksekusi program akan lebih cepat, yang berarti jumlah serangan yang dihasilkan akan lebih banyak dan membuat target mudah dilumpuhkan. Bisa juga menggunakan lebih dari satu *resources* (laptop). Menggabungkan serangan dari *resources* yang berbeda akan membuat serangan lebih kuat. Kemudian dampak serangan DOS tersebut terlihat pada target serangan yang memperlihatkan server (terminal) tidak bisa melayani dikarenakan tidak ada ‘ruang kosong’ untuk melayani.

Daftar Pustaka

[1] Miller, C. and Valasek, C., 2014. A survey of remote automotive attack surfaces. black hat USA, 2014, p.94.

[2] Kingston, L., 2018. What is an Electronic Control Unit? PH Explains. https://www.pistonheads.com/features/ph-features/what-is-an-electronic-control-unit-ph-explains/37771

[3] Alrabady, A.I. and Mahmud, S.M., 2005. Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. IEEE transactions on vehicular technology, 54(1), pp.41-50.

[4] Francillon, A., Danev, B. and Capkun, S., 2011. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS). Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

[5] Elleithy, K.M., Blagovic, D., Cheng, W.K. and Sideleau, P., 2005. Denial of service attack techniques: Analysis, implementation and comparison.

[6] Richardson, A., 2015. Security of vehicle key fobs and immobilizers.

[7] Glocker, T., Mantere, T. and Elmusrati, M., 2017, April. A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography. In Information and Communication Systems (ICICS), 2017 8th International Conference on (pp. 310-315). IEEE.

[8] Chao-yang, Z., 2011, August. DOS attack analysis and study of new measures to prevent. In Intelligence Science and Information Engineering (ISIE), 2011 International Conference on (pp. 426-429). IEEE.

[9] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S., 2010, May. Experimental security analysis of a modern automobile. In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 447-462). IEEE.

[10] Deng, J., Yu, L., Fu, Y., Hambolu, O. and Brooks, R.R., 2017. Security and Data Privacy of Modern Automobiles. In Data Analytics for Intelligent Transportation Systems (pp. 131-163).

[11] Daimi, K., Saed, M., Bone, S., Robb, J, 2016. Securing Vehicle's Electronic Control Units.

[12] Ko, C., Ruschitzka, M. and Levitt, K., 1997, May. Execution monitoring of security-critical programs in distributed systems: A specification-based approach. In Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on (pp. 175-187). IEEE.