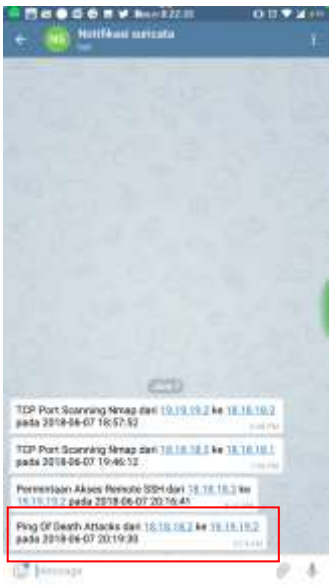
command selama 10 detik. Hasil yang diperoleh dari eksekusi *file* kirimpesan.php dapat dilihat pada Gambar 14.



Gambar 14. Tampilan pesan pada *handphone* saat terjadi ping of death

Dari gambar dapat dilihat bahwa pesan telah berhasil terkirim ke *handphone* melalui pesan instan telegram dengan selang waktu 10 detik setelah *alert* yang dihasilkan suricata berhasil masuk kedalam *database* snorby.

IV. KESIMPULAN

Skrip pengoperasian d_start pada IDS suricata sudah berhasil berjalan dengan baik sebagaimana yang diharapkan. Suricata dapat mendeteksi serangan-serangan yang masuk pada sistem dan mengirimkan *alert* nya kedalam *database* snorby. Skrip pengoperasian d_start pada snorby sudah berhasil berjalan dengan baik sebagaimana yang diharapkan, karena sudah dapat menampilkan web *interface* snorby ketika diketikkan alamat ip IDS suricata dengan port 3000 pada web browser.

Service barnyard2 telah bekerja dengan baik sebagaimana yang diharapkan karena barnyard2 sudah dapat membaca informasi yang ada pada *file* log unified2 dan mengirimkannya ke *database* snorby.

Informasi yang terkirim kedalam *database* snorby relevan dengan informasi serupa yang terdapat pada *file* fast.log dan *file* eve.json yang juga merupakan *file* untuk menampung *alert* yang dihasilkan suricata setelah berhasil mendeteksi serangan yang masuk.

Pesan pemberitahuan kepada administrator yang terdiri dari keterangan serangan, ip penyerang, ip target, dan waktu penyerangan telah berhasil terkirim ke handphone administrator melalui pesan instan telegram setelah 10 detik setelah *alert* yang dihasilkan suricata berhasil masuk kedalam *database* snorby. Dengan adanya sistem ini (yang terdiri dari IDS Suricata, Snorby, Barnyard2 dan Telegram) Administrator dapat memonitor keamanan pada jaringan yang dikelolanya melalui web *interface* snorby dan pesan pemberitahuan yang dikirimkan melalui telegram.

REFERENSI

[1] Shaik Akbar, Dr.K.Nageswara Rao, Dr.J.A.Chandula "Intrusion Detection System Methodologies Based on Data Analysis", international Journal of Computer Application(0975-8887) Volume 5-no.2, August 2010.

[2] Balaji Darapareddy and Vijayadeep Gummadi, "An Advanced Honeypot System for Efficient Capture and Analysis of Network Attack Traffic", International Journal of Engineering Trends and Technology- vol. 3, no. 5, pp.616-621, 2012.

[3] Sofyan Hadi, Periyadi,ST., M.T., Anang Sularsa, S.T., M.T. "Implementasi Network Intrusion Detection System pada Sistem Smart Identification", e-Proceeding of Applied Science – vol.2, No.3 December 2016.

[4] Park Wohyung, Ahn Seongjin., "Performance Comparison and Detection Analysis in Snort and Suricata Environment", International Journal Wireless Pers Common DOI 10.1007/s11277-016-3209-9, Springer Science, New York 2016

[5] OISF, "Suricata User Guide Release 4.0.0-dev", Suricata, July 18,2018

[6] Day, D.J. and B.M. Burns. A performance analysis of snort and suricata network intrusion detection and prevention engines. in The Fifth International Conference on Digital Society. 2011.

[7] Wibowo, R.A., "Analisis dan Implementasi IDS Menggunakan Snort pada Cloud Server di Jogja Digital Valley", Naskah Publikasi, Jurusan Teknik Informatika SMIK AMIKOM Yogyakarta, Yogyakarta, 2014.

[8] Forensic Wiki. "Barnyard2", Forensicwiki.org, 2013. https://www.forensicswiki.org/wiki/Barnyard2 (Di akses terakhir : 6 Juni 2018,12.45).

[9] Shivangi Shandilya, "Shell Scripting And Shell Programming In Unix", International Journal Of Innovative Research In Technology (IJIRT 101640), 2014.

[10] Moch Fajar, "Pengantar Pemrograman Bash Shell di Linux". Linux.or.id 2002. http://pemula.linux.or.id/programming/bash-shell.html (Di akses terakhir : 29 Agustus 2018, 21.53).

[11] Bernaeth, Nicolas., "Debian - Send your Server Notifications thru Telegram", Dyndns.org. http://bernaerts.dyndns.org/linux/75-debian/351-debian-send-telegram-notification (Di akses terakhir : 26 Okt 2017, 6:51).

[12] Hadil Deekshith., "Get Server Notification on Telegram App", Assistanz.com. https://www.assistanz.com/get-server-notification-telegram-app/ (Di akses terakhir : 27 Agustus 2018, 22:30).