

KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat beserta karunia-Nya sehingga penulis dapat menyelesaikan proyek akhir yang berjudul "SISTEM KEAMANAN PADA JARINGAN PERANGKAT IOT (INTERNET OF THINGS) RASPBERRY PI DENGAN IPTABLES DAN SYSTEM LOGIN" yang dilaksanakan di Akademi Teknik Telekomunikasi Sandhy Putra Jakarta. Penulis menyadari baik dalam tulisan maupun praktiknya, proyek akhir ini jauh dari kata sempurna, maka dari itu penulis sangat mengharapkan kritik dan saran pembaca sekalian. proyek Akhir ini juga diperuntukan untuk memenuhi salah satu syarat dalam memperoleh gelar Diploma III (Amd,T) pada Program Studi D3 Akademi Teknik Telekomunikasi Sandhy Putra Jakarta.

Penulis mengucapkan terima kasih yang sebesar-besarnya atas semua bantuan yang telah diberikan, baik secara materil maupun moril selama penyusunan proyek akhir ini hingga selesai. Secara khusus rasa terima kasih tersebut penulis sampaikan kepada:

1. Bapak Dr. Eng. Indra Chandra selaku Direktur Akademi Telkom Jakarta.
2. Bapak Suyatno, ST .,MT. Selaku Pembimbing Tugas Akhir di Akademi Telkom Jakarta.
3. Bu Ilfyantri intyas, ST.,MT. Selaku Kaprodi di Akademi Telkom Jakarta.
4. Kedua Orang Tua saya yang telah membesarkan saya dengan penuh kasih sayang serta memberikan semangat dan masukan dalam pembuatan proyek akhir ini.
5. Teman-teman seperjuangan Akademi Teknik Telekomunikasi Jakarta angkatan 2017, khususnya kelas 16 TEL 02 yang penulis banggakan, terima kasih telah memberikan warna didalam perkuliahan.

Akhir kata, atas segala kekurangan dan ketidaksempurnaan proyek akhir ini, penulis sangat mengharapkan masukan, kritik dan saran yang bersifat membangun ke arah perbaikan dan penyempurnaan untuk proyek akhir ini.

Jakarta, Juni 2020

Penulis,


DHIO RIZQI ALIM

DAFTAR ISI

| | |
|---|------|
| LEMBAR PENGESAHAN PEMBIMBING | i |
| LEMBAR PENGESAHAN PENGUJI | ii |
| PERNYATAAN BEBAS PLAGIARISME | iii |
| HALAMAN PERNYATAAN PUBLIKASI PROYEK AKHIR | iv |
| ABSTRAK | v |
| ABSTRACT | vi |
| KATA PENGANTAR | vii |
| DAFTAR ISI | viii |
| DAFTAR GAMBAR | xi |
| DAFTAR TABEL | xiii |
| BAB I PENDAHULUAN | |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Batasan Masalah | 2 |
| 1.4 Tujuan Penelitian | 2 |
| 1.5 Manfaat Penelitian | 3 |
| 1.6 Metode Penelitian | 3 |
| 1.7 Sistematika Penulisan | 4 |
| BAB II LANDASAN TEORI | |
| 2.1 Tinjauan Singkat Penelitian Terdahulu | 5 |
| 2.2 Definisi | 6 |
| 2.2.1 Pengertian Jaringan | 6 |
| 2.2.2 Two-Factor Authentication | 6 |
| 2.2.3 Apache Web Server | 7 |
| 2.2.4 PHP | 7 |
| 2.2.5 PHPMyAdmin | 8 |
| 2.2.6 MySql | 8 |
| 2.2.7 Mac Address | 8 |
| 2.2.8 Mac Address Filtering | 8 |
| 2.2.9 OTP (<i>One Time Password</i>) | 8 |
| 2.2.10 Web Server | 9 |
| 2.2.11 UDP Flood Attack | 9 |
| 2.2.12 HTTP Flood Attack | 9 |

| | |
|---|----|
| 2.2.13 CVSS (COMMON VULNERABILITY SCORING SYSTEM)..... | 9 |
| 2.2.14 Metrik Keamanan VEA-bility..... | 10 |
| 2.2.15 Network Vulnerability Dimension..... | 10 |
| 2.2.16 Network Exploitability Dimension..... | 10 |
| 2.2.17 Network Attackability Dimension..... | 11 |
| BAB III PERANCANGAN SISTEM DAN ANALISA | |
| 3.1 <i>Flowchart</i> Perancangan Sistem..... | 12 |
| 3.1.1 <i>Flowchart</i> SDLC..... | 12 |
| 3.1.2 <i>Flowchart Cara Kerja Sistem</i> | 13 |
| 3.2 Perancangan Sistem..... | 15 |
| 3.2.1 Diagram Blok..... | 15 |
| 3.2.2 Rancangan Topologi..... | 16 |
| 3.2.3 Rancangan Layout Web..... | 16 |
| 3.2.4 Rancangan Layout Tampilan..... | 17 |
| 3.2.5 Rancangan Database..... | 17 |
| 3.3 Hasil Akhir..... | 18 |
| BAB IV HASIL DAN PEMBAHASAN | |
| 4.1 Implementasi Sistem..... | 19 |
| 4.1.1 Realisasi Database Web..... | 19 |
| 4.2 Registrasi Mac Address Perangkat..... | 21 |
| 4.3 Penutupan Port..... | 22 |
| 4.4 Registrasi Akun pada web..... | 27 |
| 4.5 Login Akun pada web..... | 30 |
| 4.6 Pengujian..... | 32 |
| 4.6.1 Pengujian Mac Address Filter..... | 32 |
| 4.6.2 Pengujian System Login..... | 33 |
| 4.6.3 Pengujian serangan DoS..... | 34 |
| 4.6.4 Pengujian serangan UDP tanpa menggunakan sistem keamanan dan pertahanan..... | 35 |
| 4.6.5 Pengujian serangan HTTP tanpa menggunakan sistem keamanan dan pertahanan..... | 35 |
| 4.6.6 Pengujian serangan UDP dengan menggunakan sistem keamanan dan pertahanan..... | 35 |
| 4.6.7 Pengujian serangan HTTP dengan menggunakan sistem keamanan dan pertahanan..... | 35 |
| 4.7 Hasil Pengukuran Metrik VEA-bility..... | 36 |

| | |
|---------------------------------------|------------|
| 4.8 Hasil Pengukuran nilai CVSS | 37 |
| 4.9 Analisa | 37 |
| BAB V KESIMPULAN DAN SARAN | |
| 5.1 Kesimpulan | 39 |
| 5.2 Saran..... | 39 |
| DAFTAR PUSTAKA | xiv |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2.1. Apache | 7 |
| Gambar 3.1. Flowchart SDLC | 12 |
| Gambar 3.2. Flowchart cara kerja | 14 |
| Gambar 3.3. Diagram Blok | 16 |
| Gambar 3.3. Topologi | 16 |
| Gambar 3.4. Tampilan Layout Halaman utama | 17 |
| Gambar 3.5. Tampilan Layout Halaman Login | 17 |
| Gambar 3.6. Halaman utama | 18 |
| Gambar 4.1. database web | 19 |
| Gambar 4.2. command mac address | 20 |
| Gambar 4.3. command mac address 1 | 20 |
| Gambar 4.4. command mac address 2 | 21 |
| Gambar 4.5. command mac address 3 | 21 |
| Gambar 4.6. command mac address 4 | 21 |
| Gambar 4.7. command mac address 5 | 22 |
| Gambar 4.8. command pengecekan port | 22 |
| Gambar 4.9. install nmap | 22 |
| Gambar 4.10. command nmap | 23 |
| Gambar 4.11. nmap web | 23 |
| Gambar 4.12. penutupan port | 24 |
| Gambar 4.13. penutupan port 1 | 24 |
| Gambar 4.14. penutupan port 2 | 24 |
| Gambar 4.15. penutupan port 3 | 25 |
| Gambar 4.16. penutupan port 4 | 25 |
| Gambar 4.17. penutupan port 5 | 25 |
| Gambar 4.18. penutupan port 6 | 26 |
| Gambar 4.19. penutupan port 7 | 26 |
| Gambar 4.20. penutupan port 8 | 27 |
| Gambar 4.21. Google Authenticator | 27 |
| Gambar 4.22. Halaman Utama 1 | 28 |

| | |
|---|----|
| Gambar 4.23. Halaman Registrasi | 28 |
| Gambar 4.24. Halaman Registrasi 1 | 28 |
| Gambar 4.25. Halaman Registrasi 2 | 29 |
| Gambar 4.26. Tampilan Google Authenticator | 29 |
| Gambar 4.27. Halaman Utama 2 | 30 |
| Gambar 4.28. Halaman login | 30 |
| Gambar 4.29. Halaman login 2 | 31 |
| Gambar 4.30. Aplikasi Google Authenticator | 31 |
| Gambar 4.31. Dashboard selesai Login | 32 |
| Gambar 4.32. Pengujian Mac Address | 33 |
| Gambar 4.33. Pengujian Web Login 1 | 33 |
| Gambar 4.34. Pengujian Web Login 2 | 34 |
| Gambar 4.35. Pengujian Web Login 3 | 34 |
| Gambar 4.36. Grafik VEA-bility | 36 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 2.1. Perbandingan Penelitian | 6 |
| Tabel 3.1. Username dan password untuk Login | 17 |
| Tabel 4.1. Perbandingan nilai CVSS tiap kondisi | 37 |