

DAFTAR GAMBAR

| | |
|---|----|
| Gambar 3. 1 Blok Diagram / Topologi Sistem Saat Ini | 10 |
| Gambar 3. 2 Blok Diagram / Topologi Usulan..... | 12 |
| Gambar 3. 3 <i>Flowchart</i> Diagram Usulan | 13 |
| Gambar 4. 1 Proyek Baru | 15 |
| Gambar 4. 2 Kapasitas Memori..... | 16 |
| Gambar 4. 3 Masukkan <i>Image</i> Ubuntu 18.03 LTS..... | 16 |
| Gambar 4. 4 Pembuatan Akun..... | 17 |
| Gambar 4. 5 Pilihan Metode Instalasi | 17 |
| Gambar 4. 6 Pilihan Metode Partisi Disk | 18 |
| Gambar 4. 7 <i>Login</i> VPS..... | 18 |
| Gambar 4. 8 <i>Dashboard</i> VPS..... | 19 |
| Gambar 4. 9 Memilih Sistem Operasi | 19 |
| Gambar 4. 10 Menjalankan SSH-Console | 20 |
| Gambar 4. 11 <i>Tools Honeytrap</i> di Github | 20 |
| Gambar 4. 12 Instalasi <i>Honeytrap</i> | 21 |
| Gambar 4. 13 Laptop Pertama Sebagai Server | 23 |
| Gambar 4. 14 <i>Dashboard Honeytrap</i> | 23 |
| Gambar 4. 15 <i>Logs</i> Aktifitas Penyerang | 24 |
| Gambar 4. 16 Laptop Kedua Sebagai Penyerang..... | 24 |
| Gambar 4. 17 <i>Scanning</i> IP Address | 25 |
| Gambar 4. 18 Mencari Serangan Metode SSH-Console | 26 |
| Gambar 4. 19 Teknik Metasploit..... | 26 |
| Gambar 4. 20 Menentukan <i>IP Address</i> Target..... | 28 |
| Gambar 4. 21 Menentukan <i>Username</i> dan <i>Password</i> | 28 |
| Gambar 4. 22 Proses <i>Scanning</i> Hydra | 29 |
| Gambar 4. 23 Teknik Penyerangan SSH-Console..... | 29 |
| Gambar 4. 24 <i>Logs</i> Serangan SSH | 30 |
| Gambar 4. 25 <i>Logs</i> Serangan Nmap..... | 31 |
| Gambar 4. 26 <i>Logs</i> Serangan Metasploit..... | 31 |
| Gambar 4. 27 <i>Logs</i> Serangan Hydra..... | 31 |