

DAFTAR GAMBAR

Gambar II-1 Struktur Registry	10
Gambar III-1 Model Konseptual.....	14
Gambar III-2 Sistematika Penelitian.....	15
Gambar IV-1 Ilustrasi penyerangan.....	18
Gambar IV-2 Alur Penyerangan	21
Gambar IV-3 Baris kode menambah Exclusion	22
Gambar IV-4 Baris kode membuat file ipconfig	22
Gambar IV-5 Baris kode mengirimkan informasi jaringan melalui e-mail	23
Gambar IV-6 Baris kode untuk menambahkan registry backdoor	24
Gambar IV-7 Registry berhasil ditambahkan	24
Gambar IV-8 Baris kode untuk menonaktifkan UAC	25
Gambar IV-9 Baris kode untuk menonaktifkan restrictanonymous	25
Gambar IV-10 Ilustrasi unduh <i>file .exe</i>	26
Gambar IV-11 Baris kode mengunduh file .exe	26
Gambar IV-12 Baris kode untuk menjalankan file .exe.....	27
Gambar V-1 <i>Windows</i> Run Command Prompt Admin.....	28
Gambar V-2 Berhasil masuk ke dalam Command Prompt admin.....	29
Gambar V-3 Berhasil masuk ke mode Powershell	29
Gambar V-4 Menambahkan Exclusion pada <i>Windows</i> Defender.....	30
Gambar V-5 Keluar dari mode Powershell.....	30
Gambar V-6 Baris kode untuk membuat file yang berisi konfigurasi jaringan....	31
Gambar V-7 Mengirimkan file melalui e-mail menggunakan powershell	31
Gambar V-8 Bukti pengiriman e-mail <i>file ipconfig.txt</i>	32
Gambar V-9 Baris kode untuk masuk ke Direktori "%homepath%"	32
Gambar V-10 Berhasil masuk ke direktori "%homepath%"	32
Gambar V-11 Berhasil menambahkan Registry <i>backdoor</i>	33
Gambar V-12 Berhasil menonaktifkan UAC.....	33
Gambar V-13 Berhasil menonaktifkan restrictanonymous.....	34
Gambar V-14 Baris kode untuk mengunduh file .exe	34

Gambar V-15 Berhasil mengunduh file .exe	35
<i>Gambar V-16 Baris kode untuk menjalankan file .exe</i>	<i>35</i>
Gambar V-17 Baris kode untuk keluar dari Command Prompt.....	35
Gambar V-18 Baris kode untuk menulurkan CMD komputer target.....	36
Gambar V-19 Berhasil masuk ke CMD komputer target	36
Gambar V-20 Command untuk mengakses file komputer target	37
Gambar V-21 Mengakses <i>Public Folder</i> GUI.....	37
Gambar V-22 Akses file yang ingin diambil	38
Gambar V-23 Memindahkan <i>file</i> ke dalam komputer penyerang.....	38
Gambar V-24 Kondisi saat <i>Evilduino</i> terhubung.....	39
Gambar V-25 <i>Reverse shell</i> saat <i>Evilduino</i> terhubung	40
Gambar V-26 Backdoor yang ditanamkan masih ada setelah <i>Evilduino</i> dilepas .	41
Gambar V-27 Akses reverse shell setelah <i>Evilduino</i> sudah dilepas	41