

DAFTAR GAMBAR

Gambar II. 1 Penggunaan Meterpreter 'SMS Dump' (Royana et al., 2023).....	9
Gambar II. 2 Hasil 'Dump SMS' (Royana et al., 2023).....	9
Gambar II. 3 Hasil uji teknik <i>evasion</i> untuk <i>antivirus</i> (Samociuk, 2023)	10
Gambar II. 4 Flowchart metasploit	12
Gambar II. 5 <i>Interface msfconsole</i>	13
Gambar II. 7 Ilustrasi penggunaan <i>msfvenom</i>	14
Gambar II. 6 Flowchart penggunaan <i>msfvenom</i>	14
Gambar II. 8 Ilustrasi akses meterpreter	15
Gambar II. 9 <i>List command meterpreter</i>	15
Gambar II. 10 Ilustrasi penggunaan wireshark	17
Gambar II. 11 <i>Flowchart decision tree</i>	18
Gambar II. 12 Interface VMware	20
Gambar III. 1 Flowchart alur penelitian.....	23
Gambar III. 2 Metode yang diusulkan	26
Gambar III. 3 <i>Flowchart pembuatan malware</i>	27
Gambar III. 4 Flowchart distribusi file	29
Gambar IV. 1 Pembuatan <i>Malware: Exe</i>	40
Gambar IV. 2 <i>PDF Module</i> pada <i>Metasploit</i>	41
Gambar IV. 3 Pembuatan <i>Malware: PDF</i>	42
Gambar IV. 4 Pembuatan <i>Malware: DOC</i>	43
Gambar IV. 6 Halaman Akhir <i>DOC Original</i> (kiri) dan <i>Malware</i> (kanan).....	44
Gambar IV. 5 Halaman Awal <i>DOC Original</i> (kiri) dan <i>Malware</i> (kanan).....	44
Gambar IV. 7 Halaman Akhir <i>DOCX Original</i> (kiri) dan <i>Malware</i> (kanan)	45
Gambar IV. 8 <i>IP Address Attacker</i>	46
Gambar IV. 9 <i>Metasploit: Penggunaan Handler</i>	47
Gambar IV. 10 <i>Metasploit: Konfigurasi Handler</i>	48
Gambar IV. 11 <i>File Malware: EXE</i>	48
Gambar IV. 12 <i>Execution File Malware Line</i>	49
Gambar IV. 13 <i>File Malware: PDF</i>	50
Gambar IV. 14 <i>Execution File Malware PDF</i>	50

Gambar IV. 15 <i>File Malware: DOC</i>	51
Gambar IV. 16 <i>Execution File Malware DOC</i>	52
Gambar IV. 17 <i>File Malware: DOCX</i>	53
Gambar IV. 18 <i>Execution File Malware DOCX</i>	53
Gambar IV. 19 <i>Pembuktian Akses Meterpreter</i>	54