

DAFTAR GAMBAR

Gambar 1-1 Metode Waterfall	4
Gambar 2-1 Macam-macam Random Access Memory.....	7
Gambar 2-2 Macam-macam Sistem Operasi	8
Gambar 2-3 Diagram Alur Live Forensik	9
Gambar 3-1 Topologi Sistem Pengujian.....	13
Gambar 3-2 Bagan Logika Pengujian	16
Gambar 4-1 file config.inc DVWA Windows XP SP3.....	20
Gambar 4-2 Create / Reset Database DVWA.....	20
Gambar 4-3 Create Partition / XUbuntu	22
Gambar 4-4 Create Partition Swap Area.....	22
Gambar 4-5 Informasi User	23
Gambar 4-6 Partisi Kali Linux 2.0	25
Gambar 4-7 Nmap Scanning Host.....	26
Gambar 4-8 Halaman Login DVWA.....	27
Gambar 4-9 Security Level DVWA.....	28
Gambar 4-10 Inspect Element Maxlength	29
Gambar 4-11 URL XSS Reflected Before	29
Gambar 4-12 URL XSS Reflected After	29
Gambar 4-13 Netcut Informasi.....	30
Gambar 4-14 Tamper Data Open.....	30
Gambar 4-15 Tamper With Request.....	31
Gambar 4-16 Tamper Data Cookie	31
Gambar 4-17 Nmap Scanning Host.....	32
Gambar 4-18 Nmap scanning service	32
Gambar 4-19 Nano password.txt.....	32
Gambar 4-20 Password List	33
Gambar 4-21 Brute Force menggunakan Hydra	33
Gambar 4-22 FTP Access.....	34
Gambar 4-23 Upload file FTP.....	34
Gambar 4-24 Nmap Scanning Host.....	35
Gambar 4-25 Ifconfig Kali Linux.....	35
Gambar 4-26 Mfsconsole.....	36
Gambar 4-27 Konfigurasi Payload	37
Gambar 4-28 Sebelum Payload Berjalan	37
Gambar 4-29 Setelah Payload Berjalan	38
Gambar 4-30 Persistence Proses	38
Gambar 4-31 Command Prompt.....	39
Gambar 4-32 Informasi Image – Session Hijacking.....	41

Gambar 4-33 Informasi Pstree – Session Hijacking.....	41
Gambar 4-34 Proses Bulk Extractor	43
Gambar 4-35 Analisis Wireshark.....	44
Gambar 4-36 timeline-mactime.txt bukti mencurigakan.....	46
Gambar 4-37 mftparser bukti mencurigakan	46
Gambar 4-38 Informasi Image – Session Hijacking.....	48
Gambar 4-39 Informasi Pstree – FTP Attack.....	48
Gambar 4-40 Informasi Connscan – FTP Attack.....	49
Gambar 4-41 Informasi pslist – FTP Attack.....	49
Gambar 4-42 Proses Bulk Extractor	51
Gambar 4-43 Analisis Wireshark – FTP Attack.....	52
Gambar 4-44 Analisis Wireshark – FTP Attack.....	52
Gambar 4-45 Analisis Wireshark – FTP Attack.....	53
Gambar 4-46 timeline-mactime.txt bukti mencurigakan.....	54
Gambar 4-47 mftparser bukti mencurigakan	54
Gambar 4-48 Informasi Image – Illegal Access	56
Gambar 4-49 Informasi Pstree – Illegal Access.....	56
Gambar 4-50 Informasi Connections – Illegal Access	57
Gambar 4-51 Informasi Sockets – Illegal Access.....	57
Gambar 4-52 Informasi Pslist – Illegal Access.....	57
Gambar 4-53 Informasi privs – Illegal Access	58
Gambar 4-54 Informasi envvars – Illegal Access.....	59
Gambar 4-55 Informasi dllist – Illegal Access.....	60
Gambar 4-56 Informasi cmdscan – Illegal Access	61
Gambar 4-57 Informasi Consoles – Illegal Access.....	61
Gambar Lampiran 4-1 Tanggal dan Waktu	70
Gambar Lampiran 4-2 Disconnect Jaringan	70
Gambar Lampiran 4-3 Capture Memory.....	71
Gambar Lampiran 4-4 Browse Lokasi Penyimpanan.....	71
Gambar Lampiran 4-5 Capture Success	71