

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PENGESAHAN PEMBIMBING LAPANGAN MAGANG	ii
KATA PENGANTAR	iii
PERNYATAAN	iv
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah dan Solusi	2
1.3 Tujuan	3
1.4 Batasan Masalah	3
1.5 Penjadwalan Kerja.....	3
BAB II STUDI PUSTAKA	5
2.1 Adobe Coldfusion.....	5
2.1.1 MITRE ATT&CK ID: T1027	6
2.1.2 MITRE ATT&CK ID: T1505.003.....	6
2.1.3 MITRE ATT&CK ID: T1087.001.....	6
2.1.4 MITRE ATT&CK ID: T1069.001.....	7
2.1.5 MITRE ATT&CK ID: T1003.....	7
2.1.6 MITRE ATT&CK ID: T1562.004.....	8
2.1.7 MITRE ATT&CK ID: T1021.001.....	8
2.1.8 MITRE ATT&CK ID: T1112.....	8
2.1.9 MITRE ATT&CK ID: TA0004	9
2.2 Perusahaan CTI Group	9
2.3 Gambaran Umum Institusi	11
2.4 Divisi Kerja.....	14
BAB III ANALISIS PEKERJAAN	17
3.1 Deskripsi dan Alur Pekerjaan	17

3.2	Analisis <i>Adobe ColdFusion Exploit Lead to System Compromise</i>	18
3.2.1.	Analisa Pada Server 1.....	19
3.2.1.1	<i>File Creation (MITRE ATT&CK ID: T1027)</i>	19
3.2.1.2	<i>Server Software Component (MITRE ATT&CK ID: T1505.003)</i>	19
3.2.1.3	<i>Local Account (MITRE ATT&CK ID: T1087.001)</i>	20
3.2.1.4	<i>Local Groups (MITRE ATT&CK ID: T1069.001)</i>	22
3.2.1.5	<i>OS Credential Dumping (MITRE ATT&CK ID: T1003)</i>	22
3.2.1.6	<i>Upload Tool (MITRE ATT&CK ID: T1608.002)</i>	23
3.2.1.7	<i>Disable or Modify System Firewall (MITRE ATT&CK ID: T1562.004)</i>	23
3.2.1.8	<i>Windows Registry (MITRE ATT&CK ID: DS0024)</i>	24
3.2.1.9	<i>Upload Tool (MITRE ATT&CK ID: T1608.002)</i>	24
3.2.1.10	<i>OS Credential Dumping (MITRE ATT&CK ID: T1003)</i>	25
3.2.1.11	<i>LSASS Memory (MITRE ATT&CK ID: T1003.001)</i>	25
3.2.1.12	<i>Domain Groups (MITRE ATT&CK ID: T1087)</i>	25
3.2.1.13	<i>Remote Desktop Protocol (MITRE ATT&CK ID: T1021.001)</i>	26
3.2.1.14	<i>Privilege Escalation (MITRE ATT&CK ID: TA0004)</i>	26
3.2.2.	Analisa Pada Server 2.....	27
3.2.2.1	<i>Server Software Component (MITRE ATT&CK ID: T1505.003)</i>	27
3.2.2.2	<i>Ingress Tool Transfer (MITRE ATT&CK ID: T1105)</i>	28
3.2.2.3	<i>OS Credential Dumping (MITRE ATT&CK ID: T1003)</i>	29
3.2.2.4	<i>Data from Local System (MITRE ATT&CK ID: T1005)</i>	29
3.2.2.5	<i>Non-Application Layer Protocol (MITRE ATT&CK ID: T1095)</i>	29
3.2.2.6	<i>Windows Admin Shares (MITRE ATT&CK ID: T1021.002)</i>	29
3.2.2.7	<i>Protocol Tunneling (MITRE ATT&CK ID: T1572)</i>	30
3.2.2.8	<i>Discovery (MITRE ATT&CK Tactic ID: TA0007)</i>	30
3.2.2.9	<i>SMB/Windows Admin Shares (MITRE ATT&CK ID: T1021.002)</i>	30
3.2.2.10	<i>OS Credential Dumping (MITRE ATT&CK ID: T1003.002)</i>	31
3.2.2.11	<i>Network Share Connection Removal (MITRE ATT&CK ID: T1070.005)</i>	31
3.3	Kebutuhan Perangkat Kerja	32
BAB IV HASIL DAN PEMBAHASAN		37
4.1	Hasil Akhir (Luaran).....	37

4.2	Dampak <i>Server Compromised</i>	40
BAB V KESIMPULAN DAN SARAN		43
5.1	Kesimpulan.....	43
5.2	Saran	43
DAFTAR PUSTAKA		45
LAMPIRAN		47