



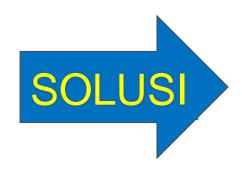






Latar Belakang Perusahaan

- 1. PT. Putra Mulia Telecomunication (PMT) Berdiri Tahun 2011
- 2. PT. PMT Menjadi Anak Perusahaan OCK Group Tahun 2014



- Memberikan jasa Operasi dan Pemeliharaan Jasa Outsourcing dibidang Telecomunication. Dengan konsep mengadopsi metodologi Industri terbaik (best Practise) serta sumber daya yang terampil untuk memastikan kinerja yang unggul
- 2. Pelayanan Roll-Out Deployment Jaringan
- 3. Solusi dan Layanan FTTX/ FTTH
- 4. Optimasijaringan Radio.

Visi:

To be visionary leader in delivering the best telecommunication services to enrich lives

Misi:

We will dedicate ourselves to provide high value and beneficial solutions, an excellence services exceeding our customer's expectation

Bridging Success for Your Business



- 1. Adanya keinginan perusahaan untuk mengetahui celah keamanan dari aplikasi web (company profile) yang saat ini & Infrastructre berjalan,
- 2. Selain itu juga ingin mengetahui apakah sistem aplikasi web ini memenuhi aspek sistem manajemen keamanan informasi (aspek Confidentiality, Integrity dan Availability)
- 3. Hasil dari pelaksanaan Vulnerability Asesment ini sebagai dasar untuk perbaikan sistem manajamen keamanan informasi aplikasi web yang ada pada Perusahaan.





Latar Belakang Pentest PT. Putra Mulia Telecomunation

No	Item	Qty									
Infr	Infrastructure										
1	Firewall Fortigate (IP Publik)	1									
2	Router Mikrotik (IP Publik)	1									
3	NAS Synology (IP Publik)	1									
Aplil	Aplikasi Website										
1	Web Application Company Profile (External Hosted)	1									





- Metode Pentest



Pentest Aplikasi web dan mobile:

- Information Gathering dan Vulnerability Identification, meliputi:
- 1. Pentest Server

Penetration test server

Pengujian serangan:

- Vulnerability Assessment, meliputi:
- Information gathering
- Check port open / close
- Check software version
- OS fingerprinting
- Weak password / authentication
- Check vulnerability Software
- Check SSL configuration (jika menggunakan protokol ssl)
- Exploitation & Post-Exploitation, meliputi:
- Attack / security testing terhadap temuan pada vulnerability assessment.

Penetration test aplikasi web

Target: -

catatan jika Grey Box:

Diperlukan 2 user dummy (1 user dengan level rendah dan 1 user dengan level admin) untuk melakukan pentest

Pengujian serangan:

- Input and Data Validation, meliputi:
- Cross Site Scripting (XSS)
- SQL injection
- Authorization, meliputi:
- Bypassing authorization schema
- Insecure Direct Object References
- Session Management, meliputi:
- Session Management schema
- Cookies attributes
- Broken Authentication
- Check SSL configuration (jika menggunakan protokol ssl)



- Rencana Kerja



No	Aktivitas		Month 1										Month 2																					
				W1				W2				W3				W4					W5			W6				W7				W8		
1	Tahap 1: Planing																														T		П	
1.1	Pembahasan Skope				Г		П	Τ	Т			Т	Τ			П	П		Т	Г			Т	Г	П	П	T	Т	Γ	П	Т	T	П	\neg
1.2	Pengumpulan Data-2 (<u>Visi</u> Misi, Struktur Organisasi, User Dumy)																																	
1.3	Kick Off				Γ	П		Τ	Т		T	Т	Τ	Τ		П	П	T	Т	П	П	T	Τ	Г	П	\sqcap	T	T	Г	П	T	T	П	٦
2	Tahap 2: Penetration Test , Infrastructure Assesment & Data Collection																																	
2.1	Vunerability Assesment <u>Infrastruktur</u> (Firewall Fortigate, NAS)																																	
2.3	Vulnerabiltiy Web Application Company Profile																																	
3	Tahap 3: Re-Penetration Test																																	
3.1	Vunerability Assesment <u>Infrastruktur</u> (Firewall Fortigate, NAS)																																	
3.3	Vulnerabiltiy Web Application Company Profile																																	
4	Tahap 4: Reporting																																Ш	
4.1	Laporan Hasil Vulnerability Assessment Instrasturktur																																	
4.2	Laporan <u>Hasil Penetration</u> Test & Re Penetration Test Web Application																																	
4.3	Laporan Final																																\prod	
5	Project Control																																	
5.1	Presentasi Hasil Penetration Test																																\prod	
5.2	BAST (Berita Acara Serah Terima Pekeriaan)																																	



List Form Pre Assesment

Pra Penetratio	n Test Form														
CATEGORY: WE	CATEGORY: WEB APPLICATION														
No.	IP Address/URL/Domain	Total Object	Total Page/Fungsi	Blackbox/Greybox/Whitebox	Credential										
1															
2															
3															
4															
CATEGORY: SER	VER														
No.	IP Address	Total Object	Blackbox/Greybox/Whitebox	Credential											
1															
2															
3															
4															
CATEGORY: NET	rwork														
No.	IP Address	Total Object	Blackbox/Greybox/Whitebox	Credential											
1															
2															
3															
4															
CATEGORY: OTI															
No.	IP Address	Total Object	Total Page/Fungsi	Blackbox/Greybox/Whitebox	Credential										
1															
2															
3															
4															





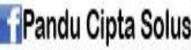




Butuh Informasi lebih lanjut?



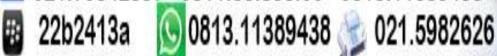
info@panducipta.com Pandu Cipta Solusi





3 021.70342357 - 0811.88.333.00 - 0813.11389438









Address

Jl. Masjid Darul Ulum Rt. 01c/ 01 no3 lantai 2, Kel. Kadu, Kec. Curug, Kab. Tangerang, Banten 15810

Gedung Menara 165, lantai 4, Jl. Cilandak Timur, Kav. 1, Jakarta Selatan - 12560

Phone Email

+62 21 598.2626 - 0811.88.333.00 - 0856.88.333.00 - 0877.8206.7171

info@panducipta.com

http://www.panducipta.com Website



Bridging Success for Your Business