Lampiran 1 : Lampiran Pedoman Wawancara

Teori/Konsep	Indikator	Pertanyaan
Teori Sixware Network Security Framework (SWNSF)	Faktor Manusia (*Brainware*)	Apakah Pusat Pertahanan Siber (Pushansiber) sampai saat ini melakukan pengembangan sumber daya manusia agar dapat menciptakan SDM yang mampu mengurangi atau bahkan menghentikan serangan ancaman siber di Indonesia dalam membangun sistem siber? Apakah dari Pushansiber Kementerian Pertahanan juga sudah memanfaatkan sumber daya manusia di Indonesia dalam penguasaan dan membangun sistem siber? Bagaimana kondisi dan bentuk pengembangan pelatihan pada pengembangan sumber daya manusia di bidang siber? Di Pushansiber sendiri telah membentuk CSIRT untuk dapat mengidentifikasi, melindungi, mendeteksi, merespon adanya serangan siber, apakah dari kegiatan tersebut telah melibatkan sdm yang

		sudah diberikan pelatihan oleh pushansiber sendiri? Apakah ada kendala atau faktor dalam pengembangan kemampuan pada sumber daya manusia dalam membangun sistem siber di pushansiber? Apakah sumber daya manusia yang dimiliki oleh Indonesia sudah memenuhi atau memiliki kemampuan atau penguasaan di bidang siber yang mana bahwa bentuk ancaman siber semakin berkembang?
	Perangkat Keras (*Hardware)*	Apakah Pushansiber Kementerian Pertahanan telah bekerjasama dengan *stakeholder* lainnya dalam meng-*upgrade* dan meningkatkan pada perangkat keras agar dapat membangun sistem siber? Bagaimana dalam meng-upgrade dan meningkatkan sistem siber di Pushansiber? Apakah Pushansiber Kementerian Pertahanan sampai saat ini melakukan pengembangan pada perangkat keras yang mampu mengurangi atau bahkan menghentikan serangan ancaman

		siber? Apakah Pushansiber Kementerian Pertahanan dan sudah memanfaatkan pengembangan perangkat keras untuk sistem sibernya sendiri? Bagaimana kondisi perangkat keras yang di miliki Pushansiber untuk sistem sibernya? Apakah sudah terpenuhi pada perangkat kerasnya? Apakah ada kendala atau faktor dalam pengembangan perangkat keras di bidang siber? Apakah perangkat keras yang dimiliki oleh Pushansiber sudah memenuhi dan memiliki kemampuan atau penguasaan di bidang siber yang mana bahwa bentuk ancaman siber semakin berkembang? Perangkat keras apa yang dipakai oleh Pushansiber Kementerian Pertahanan untuk sistem sibernya dan contohnya seperti apa? Apakah perangkat keras yang sudah jelaskan tadi di contohnya di pakai dan dapat mendukung oleh Pushansiber dalam team atau kegiatan CSIRT?

	Perangkat lunak (*software),*	Apakah Pushansiber Kementerian Pertahanan telah bekerjasama dengan *stakeholder* lainnya dalam meng-*upgrade* dan meningkatkan pada *software* agar dapat membangun sistem siber? Bagaimana dalam meng-upgrade dan meningkatkan sistem siber di Pushansiber pada sistem *software*? Apakah Pushansiber sampai saat ini melakukan pengembangan pada *software* yang mampu mengurangi atau bahkan menghentikan serangan ancaman siber? Apakah Pushansiber Kementerian Pertahanan dan sudah memanfaatkan pengembangan *software* untuk sistem sibernya sendiri? Bagaimana kondisi *software* yang di miliki Pushansiber untuk sistem sibernya? Apakah sudah terpenuhi pada *software*? Apakah ada kendala atau faktor dalam pengembangan *software* di bidang siber? Apakah perangkat keras yang dimiliki oleh Pushansiber sudah

		memenuhi dan memiliki kemampuan atau penguasaan di bidang siber yang mana bahwa bentuk ancaman siber semakin berkembang? *Software* apa yang dipakai oleh Pushansiber untuk sistem sibernya dan contohnya seperti apa? Apakah *software* yang sudah jelaskan tadi pada contohnya yang di pakai dapat mendukung Pushansiber dalam team atau kegiatan CSIRT nya?
	Perangkat infrastruktur (*infrastructure)*	Apakah Pushansiber Kementerian Pertahanan sampai saat ini melakukan pengembangan pada perangkat infrastruktur yang mampu mengurangi atau bahkan menghentikan serangan ancaman siber? Apakah Pushansiber Kementerian Pertahanan sudah memanfaatkan pengembangan perangkat infrastruktur untuk sistem sibernya? Bagaimana kondisi perangkat infrastruktur yang di miliki Pushansiber untuk sistem sibernya? Apakah ada kendala atau

		faktor dalam pengembangan perangkat infrasruktur di bidang siber untuk sistem nya? Apakah perangkat infrastruktur yang dimiliki oleh Pushansiber sudah memenuhi dan memiliki kemampuan atau penguasaan di bidang siber yang mana bahwa bentuk ancaman siber semakin berkembang? Apabila belum, mengapa dan bagaimana solusi nya? Perangkat infrastruktur apa yang dipakai oleh Pushansiber untuk sistem sibernya?
		Bagaimana dan apa saja kendala dalam kerjasama firmware untuk dapat membangun sistem siber dapat berjalan dengan semestinya? Apakah Pushansiber sampai saat ini melakukan pengembangan *Firmware* agar dapat membantu dan mampu bekerja dalam mengurangi atau bahkan menghentikan serangan ancaman siber di Indonesia dalam penggunaan sistem sibernya? Apakah Pushansiber sudah

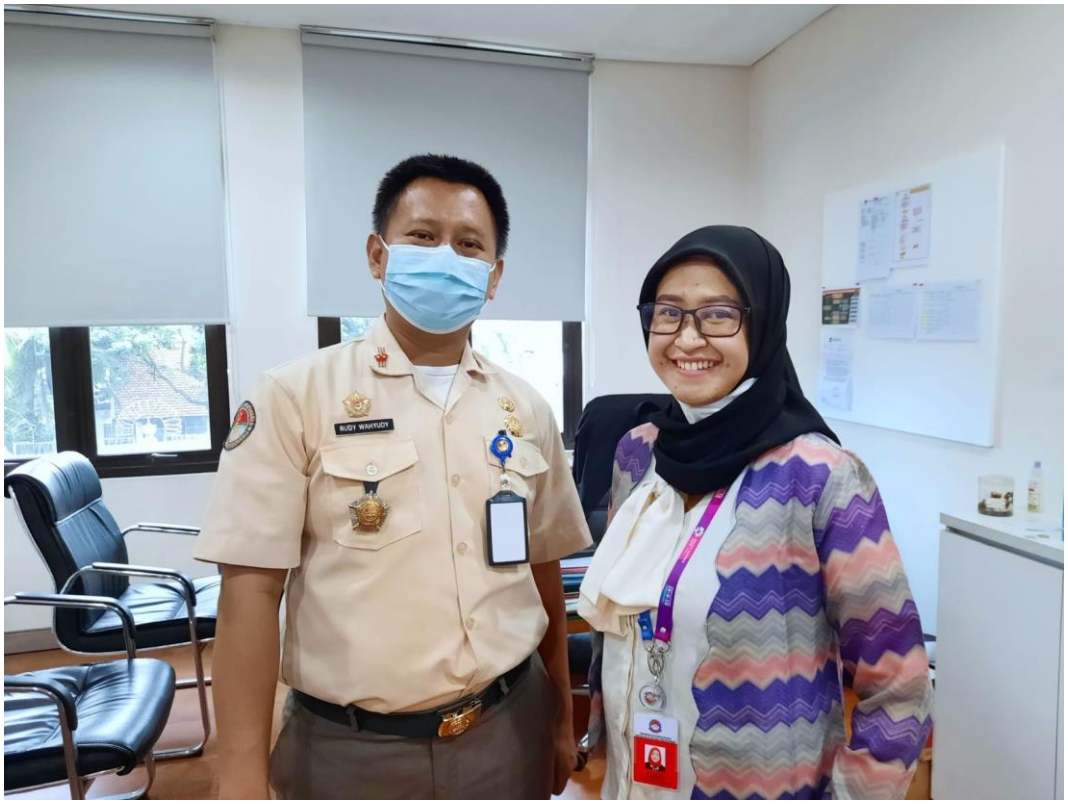
	Firmware	memanfaatkan pengembangan dan meng-update Firmware untuk membangun sistem siber? Berapa banyak anggaran yang dibutuhkakn untuk dapat meng-*update Firmware* untuk sistem siber di Pushansiber? Bagaimana kondisi dan bentuk pengembangan firmware yang dipakai oleh Pushansiber? Apakah ada kendala atau faktor dalam pengembangan kemampuan pada *Firmware* di bidang sistem siber? Apakah *Firmware* yang dimiliki oleh Pushansiber sudah memenuhi atau memiliki kemampuan atau penguasaan di bidang siber yang mana bahwa bentuk ancaman siber semakin berkembang? *Firmware* yang dipakai oleh Pushansiber pada saat ini?
		Apakah ada permasalahan mengenai anggaran di Pushansiber demi membangun sistem siber? Bagaiaman kondisi pendistribusian anggaran dari tiap bidang pengembangan sumber daya

	Anggaran (*Budgeting).*	manusia, perangkat keras, perangkat lunak, perangkat infrastruktur dan firmware menyeluruh guna memenuhi kebutuhan dalam membangun sistem siber dan menghindari adanya ketimpang tindihan? Apakah Pushansiber memfokuskan anggaran untuk dapat melakukan investasi atau pengembangan dan meng-*update* sistem sibernya? Bagaimana strategi Pushansiber dalam mengupayakan untuk memenuhi kebutuhan dalam bidang pengembangan sumber daya manusia, perangkat keras, perangkat lunak, perangkat infrastruktur, firmware yang masih dalam proses pengembangan?

Lampiran 2 Lampiran Wawancara

A. DOKUMENTASI WAWANCARA

Gambar Lampiran 1.1 Wawancara bersama Bapak Irfan Mountini, S. Kom yang memiliki jabatan sebagai Pranata Komputer Madya Pusat Pertahanan Siber, Bapak Rudy Wahyudi, S. Kom., M. Han yang memiliki jabatan sebagai Kepala Subbidang Keamanan Infrastruktur dan Komputer Bidang Penjamin Keamanan Pusat Pertahanan Siber dan Bapak Eko Joko Murwanto, S. Kom., M.Si yang memiliki jabatan sebagai Kepala Subbidang Keamanan Aplikasi Bidang Penjamin Keamanan Pusat Pertahanan Siber sebagai informan dalam penelitian ini.



Gambar Lampiran 1.2 Wawancara bersama Bapak Rudy Wahyudi, S. Kom., M. Han yang memiliki jabatan sebagai Kepala Subbidang Keamanan Infrastruktur dan Komputer Bidang Penjamin Keamanan Pusat Pertahanan Siber

Gambar Lampiran 1.3 Wawancara bersama Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc., MBA., Mphil. MA yang memiliki jabatan sebagai pakar teknologi informatika.

Gambar Lampiran 1.4 Wawancara bersama Bapak Dr. Ir. Achmad Farid W, M sebagai dosen di perguruan tinggi Universitas Pertahanan Republik Indonesia sekaligus mantan dari Kepala Cyber Defense Pusat Data dan Informasi Kementerian Pertahanan

Riwayat hidup peneliti

Nur Arifina, lahir di Jakarta pada 04 Juli 1996. Anak pertama dari 2 bersaudara. Menyelesaikan pendidikan SDN Sudimara 07 Ciledug pada 2008, menyelesaika pendidikan di SMP Negeri 219 Jakarta Barat tahun 2011 dan lulus dari SMAN Negeri 101 Jakarta Barat pada tahun 2014, pada tahun 2014 juga melanjutkan studi strata satu dan lulus pada tahun 2018 dari Universitas Budi Luhur, dan pada tahun 2020 melanjutkan program magister (S2) di Program studi Peperangan Asimetris, Fakultas Strategi Pertahanan Universitas Pertahanan.