MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 23 TAHUN 2022
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER, DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG UJI KEAMANAN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 31 Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer, dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Uji Keamanan Siber;

b. bahwa Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer, dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Uji Keamanan Siber telah disepakati melalui Konvensi Nasional pada 25 November 2021 di Jakarta;

c. bahwa sesuai surat Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi Nomor 4708/BSSN/D1/PP.01.06/12/2021 tanggal 07 Desember 2021 perihal permohonan Penetapan Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer, dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Uji Keamanan Siber;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Keputusan Menteri Ketenagakerjaan tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer, dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Uji Keamanan Siber;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 39, Tambahan Lembaran Negara Republik Indonesia Nomor 4279);

2. Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

3. Peraturan Pemerintah Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4637);

4. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);

5. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);

6. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);
7. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);
8. Peraturan Menteri Ketenagakerjaan Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Ketenagakerjaan (Berita Negara Republik Indonesia Tahun 2021 Nomor 108);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI KETENAGAKERJAAN TENTANG PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER, DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG UJI KEAMANAN SIBER.

KESATU : Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer, dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Uji Keamanan Siber, sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh dan/atau kementerian/lembaga teknis terkait sesuai dengan tugas dan fungsinya.

KEEMPAT : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dikaji ulang setiap 5 (lima) tahun atau sesuai dengan kebutuhan.

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 14 Maret 2022

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 23 TAHUN 2022
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG UJI KEAMANAN SIBER

BAB I
PENDAHULUAN

A. Latar Belakang

Guna meminimalisir terjadinya insiden siber secara nasional, Badan Siber dan Sandi Negara (BSSN) melakukan pemantauan anomali trafik terhadap Indonesia selama 24 (dua puluh empat) jam sehari dan 7 (tujuh) hari dalam seminggu. Berdasarkan statistik hasil pemantauan pada tahun 2020, ditemukan sebanyak 495.337.202 (empat ratus sembilan puluh lima juta tiga ratus tiga puluh tujuh ribu dua ratus dua) serangan siber yang ditujukan ke Indonesia. Anomali lalu lintas jaringan tertinggi terjadi pada tanggal 10 Desember 2020 dengan jumlah serangan sebanyak 7.311.606 (tujuh juta tiga ratus sebelas ribu enam ratus enam).

Selain data di atas, *Nippon Telegraph and Telephone Corporation* (NTT) menerbitkan 2021 *Global Threat Intelligence Report*. Pada laporan tersebut, tercatat bahwa keuangan adalah industri yang paling banyak diserang yang mendominasi 23% (dua puluh tiga persen) dari semua serangan selama tahun 2020. *Application specific attack* (serangan terhadap aplikasi khusus) terus terhitung mendominasi sebesar 42% (empat puluh dua persen) dari semua serangan. Sementara itu, *web application attack* (serangan terhadap aplikasi berbasis web) terjadi sebesar 31% (tiga puluh satu persen) dari semua serangan terhadap sektor keuangan. Secara rinci, persentase serangan yang terjadi pada berbagai sektor industri secara global dapat dilihat pada Tabel 1.

Tabel 1. Persentase Serangan dan Jenis Serangan pada Sektor Industri secara Global[1]

Industri dan Persentase Serangan Global	Persentase Jenis Serangan pada Industri
Keuangan – 23%	Aplikasi khusus – 42% Aplikasi berbasis web – 31% Pengintaian – 12%
Manufaktur – 22%	Aplikasi khusus – 49% Pengintaian – 24% Aplikasi berbasis web – 20%
Kesehatan – 17%	Aplikasi berbasis web – 59% Aplikasi khusus – 38% *Known bad source* – 1%
Bisnis dan jasa profesional – 10%	Pengintaian – 53% Aplikasi khusus – 13% *Brute force* – 12%
Pendidikan – 6%	Aplikasi berbasis web – 24% Aplikasi khusus – 22% Pengintaian – 21%

Tingginya serangan yang diarahkan pada aplikasi khusus dan aplikasi berbasis *web* menunjukan banyaknya kerentanan pada aplikasi maupun *website* yang digunakan. Karenanya, dapat disimpulkan bahwa faktor keamanan siber merupakan salah satu faktor terpenting dalam pengembangan teknologi atau sistem informasi.

Keamanan siber (*cybersecurity*) adalah segala aktivitas, proses, dan teknologi yang digunakan untuk melakukan pengamanan dan perlindungan kerahasiaan, integritas, dan ketersediaan informasi atau sumber daya teknologi informasi di dunia siber. Tidak dapat dipungkiri bahwa informasi merupakan salah satu aset berharga dalam sebuah organisasi yang harus dilindungi dari berbagai ancaman, baik itu yang berasal dari internal maupun eksternal.

Salah satu metode yang dapat diterapkan dalam menjamin keberlangsungan pengelolaan dan keamanan pada sistem informasi adalah dengan melaksanakan Uji Keamanan Siber (UKS). UKS bertujuan

[1] Nippon Telegraph and Telephone Corporation, 2021 *Global Threat Intelligence Report*

untuk menemukan ada atau tidaknya celah kerentanan yang dapat dieksploitasi dalam suatu serangan siber. Beberapa metodologi dan standar yang umum digunakan UKS, antara lain: *Open Source Security Testing Methodology Manual* (OSSTMM), *Penetration Testing Execution Standard* (PTES), 4.2.1 *Payment Card Industry Data Security Standard* (PCI DSS) *Penetration Testing Guide, Information System Security Assessment Framework* (ISSAF) dan *Open Web Application Security Project* (OWASP) *Testing Guide.*

Industri yang berhubungan dengan kegiatan pengujian keamanan siber juga berkembang dengan pesat. Terdapat beberapa profesi yang berkaitan dengan kegiatan pengujian keamanan siber diantaranya adalah *Vulnerability Assessment Analyst, Pentester, Red Team,* dan *Bug Bounty Hunter*.

Red Team adalah sebuah tim yang bertugas untuk melakukan simulasi serangan untuk menguji sejauh mana sebuah organisasi dapat bertahan menghadapi serangan yang dapat dilakukan oleh pelaku serangan siber secara riil. Kegiatan pengujian seperti ini tidak hanya melibatkan kegiatan simulasi serangan terhadap aset teknologi informasi secara jarak jauh, tapi juga melibatkan kegiatan pengujian perimeter keamanan fisik aset teknologi informasi tersebut dan juga pengujian secara rekayasa sosial atas aspek manusia.

Profesi di luar organisasi berkembang dalam model konsultan atau perorangan. *Vulnerability Assessment Penetration Testing* (VAPT) merupakan bagian pengujian yang didesain pada batasan ruang lingkup dan waktu, sementara model *Bug Bounty Hunter* cenderung lebih lepas dari batasan tersebut. Pada prinsipnya kegiatan *bug bounty* adalah sama dengan kegiatan uji penetrasi, yaitu melakukan simulasi serangan terhadap aset teknologi informasi dengan melakukan eksploitasi atas kerentanan yang ada pada aset tersebut, perbedaan hanyalah terkait ruang lingkup dan kerangka waktu serta kedalaman intensitas pengujian.

Keduanya menjadi sarana organisasi untuk melakukan pengujian resiko kerentanan, menutup lubang kerentanan, dan memperbaiki postur keamanan sibernya. Akan tetapi satu hal yang harus diperhatikan terkait dengan *Bug Bounty Hunter* adalah aspek legal formal dari kegiatan

tersebut. Kegiatan *Bug Bounty* yang dilakukan tanpa seizin dari pemilik aset teknologi informasi adalah kegiatan yang melanggar hukum, yaitu Pasal 30 ayat 1, ayat 2, dan atau ayat 3 Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE).

Atas dasar pertimbangan di atas, BSSN mendorong upaya untuk membangun skema kompetensi dalam pelaksanaan pengujian keamanan siber yang akan diterima secara luas oleh dunia usaha dan dunia industri. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Uji Keamanan Siber disusun sebagai panduan bagi organisasi dalam melaksanakan pengujian keamanan siber, baik di sektor pemerintahan maupun swasta.

Tersedianya standar kompetensi kerja merupakan salah satu bagian penting yang harus disiapkan dalam pengembangan sumber daya manusia secara berkualitas. Standar kompetensi kerja pada dasarnya merupakan gambaran atau informasi tentang pengetahuan, keterampilan dan sikap yang harus dimiliki untuk melaksanakan suatu tugas atau pekerjaan sebagaimana dipersyaratkan.

B. Pengertian

1. Keamanan siber adalah segala aktivitas, proses, dan teknologi yang digunakan untuk melakukan pengamanan dan perlindungan kerahasiaan, integritas, dan ketersediaan informasi atau sumber daya teknologi informasi di dunia siber.
2. Uji Keamanan Siber (UKS) adalah kegiatan pengujian terhadap perimeter keamanan siber dari sebuah organisasi dengan metode yang bersifat *offensive,* dan diselenggarakan berdasarkan ruang lingkup serta standar tertentu serta atas persetujuan pemilik aset teknologi informasi.
3. Penguji adalah personel yang memiliki pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan untuk melakukan pengujian keamanan siber.
4. Aset Teknologi Informasi atau Aset TI adalah segala hal yang berkaitan dengan informasi, perangkat keras, perangkat lunak dan

sumber daya manusia yang bernilai dan bermanfaat untuk mencapai tujuan perusahaan/organisasi. Aset perangkat keras dapat mencakup *workstation, server* dan komponennya, perangkat jaringan, *printer*, *smartphone*, *desktop, laptop* dan lain-lain, sedangkan aset perangkat lunak dapat mencakup lisensi, aplikasi, *Operating System* (OS), dan lain-lain.

5. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan suatu Aset TI.
6. Sistem skor adalah penilaian akhir dari hasil pengujian keamanan siber.
7. Informasi sensitif adalah informasi yang tidak boleh diketahui publik, contohnya kredensial, nama pengguna, direktori sistem, dan sebagainya.
8. Ruang lingkup pengujian keamanan siber adalah cakupan objek yang akan dilakukan pengujian keamanan siber, tujuan pengujian serta kerangka waktu pengerjaan pengujian tersebut.
9. Objek pengujian adalah segala hal yang berkaitan dengan sistem layanan, proses sistem layanan, infrastruktur, sistem internal, *embedded devices*, manusia dan lain-lain. Contoh dari objek pengujian tersebut diantaranya adalah *web application, mobile application,* basis data*, Internet of Thing* (IoT), *Industrial Control System* (ICS), dan lain-lain.
10. Kerangka waktu pada ruang lingkup pengujian keamanan siber adalah segala hal yang berkaitan dengan waktu yang diperlukan untuk melaksanakan pengujian, mitigasi, uji ulang, serta pembuatan laporan.
11. Tujuan pengujian adalah serangkaian kondisi atau sasaran yang ditetapkan menjadi capaian yang harus dipenuhi dalam kegiatan UKS.

C. Penggunaan SKKNI

Standar Kompetensi dibutuhkan oleh beberapa lembaga/institusi yang berkaitan dengan pengembangan sumber daya manusia, sesuai dengan kebutuhan masing-masing:

1. Untuk institusi pendidikan dan pelatihan
    a. Memberikan informasi untuk pengembangan program dan kurikulum.
    b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.
2. Untuk dunia usaha/industri dan penggunaan tenaga kerja
    a. Membantu dalam rekrutmen.
    b. Membantu penilaian unjuk kerja.
    c. Membantu dalam menyusun uraian jabatan.
    d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.
3. Untuk institusi penyelenggara pengujian dan sertifikasi
    a. Sebagai acuan dalam merumuskan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya.
    b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Uji Keamanan Siber Ditetapkan melalui Keputusan Kepala Badan Siber dan Sandi Negara Nomor 394.1 Tahun 2021 tentang Pembentukan Komite, Tim Perumus, Tim Verifikasi, dan Sekretariat Penyusunan Standar Kompetensi Kerja Nasional Indonesia Area Fungsi Keamanan Siber Tahun Anggaran 2021 tanggal 1 Oktober 2021 dapat dilihat pada Tabel 2, Tabel 3, dan Tabel 4.

Tabel 2. Susunan komite standar kompetensi SKKNI Bidang Uji Keamanan Siber

NO	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Dono Indarto, S.IK., M.H.	Badan Siber dan Sandi Negara	Pengarah
2.	Mohamad Ikro, S.Si., M.Si.	Badan Siber dan Sandi Negara	Ketua
3.	Asri Setyowati, S.Si., M.M.	Badan Siber dan Sandi Negara	Sekretaris
4.	Wida Sandrayanti, S.E.	Badan Siber dan Sandi Negara	Anggota
5.	Soetedjo Joewono, S.E, M.M.	Badan Siber dan Sandi Negara	Anggota
6.	M.Novel Ariyadi, S.T., MPM, CDPSE	Indonesia Cyber Security Forum (ICSF)	Anggota
7.	Dr. Ayi Purbasari, M.T.	Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM)	Anggota

Tabel 3. Susunan Tim Perumus SKKNI Bidang Uji Keamanan Siber

NO	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Ir. Budi Rahardjo, M.Sc., Ph.D.	Institut Teknologi Bandung	Pengarah
2.	Royke Tobing, GWAPT, GCIH, CITP	PT Spentera	Ketua
3.	Satriyo Wibowo, S.T., MBA, M.H., IPM, CERG, CCISO, SBP, CSA, ECIH, CEI	Indonesia Cyber Security Forum	Sekretaris
4.	Thomas Gregory, OSCP, OSCE, OSEE, ISO 27001-LA, GCIA	PT Spentera	Anggota
5.	Semi Yulianto, S.E., M.Kom., SSCP, CISSP, CSSLP, CISA, CISM, CASP+	PT SysTech Global Informasi (SGI Asia)	Anggota
6.	Atik Pilihanto, JNCIP-SEC, TOGAF, GSEC, GCIH, GCIA, GPEN	Cyber Defense Indonesia (CDEF)	Anggota
7.	Rahmat Nurfauzi, OSCP, CRTE, CRTO, eCPTXv2, eCTHPv2, CTI	PT Xynexis International	Anggota
8.	Girindro Pringgo Digdo, S.Kom., M.T., CSXF, OSC	Cyber Army Indonesia	Anggota
9.	Digit Oktavianto, GCIH, GMON, GCFE, GICSP, CEH, ECSA, CSA, CTIA, ECIH, CHFI, ECSS	Cyber Defense Indonesia (CDEF)	Anggota
10.	Faizal Achmad, S.Kom. M.T.	Badan Siber dan Sandi Negara	Anggota
11.	Sandromedo Christa Nugroho, S.ST., M.Han.	Asosiasi Fungsional Sandiman Indonesia	Anggota

Tabel 4. Susunan Tim verifikasi SKKNI Bidang Uji Keamanan Siber

NO	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Ir. Siswanto, M.M., M.Kom.	Universitas Budi Luhur/Ikatan Ahli Informatika Indonesia (IAII)	Ketua
2.	Anas Hilal, S.Pd.	Badan Siber dan Sandi Negara	Anggota
3.	Mita Pramihapsari, S.ST.MP	Badan Siber dan Sandi Negara	Anggota
4.	Sophia Clara Beauty Kusumawardhani, S.H.	Badan Siber dan Sandi Negara	Anggota

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Memberikan informasi berbasis hasil pengujian keamanan siber yang dibutuhkan oleh pemangku kepentingan untuk perbaikan postur keamanan organisasi	Mendesain strategi pengujian keamanan siber	Menyusun prosedur uji keamanan siber	Merencanakan prosedur uji keamanan siber
			Menentukan metode penilaian kerentanan
		Menyiapkan kebutuhan pengujian keamanan siber	Menentukan ruang lingkup pengujian keamanan siber
			Menentukan tim penguji keamanan siber
	Memeriksa keamanan siber	Menghimpun informasi yang relevan dengan ruang lingkup pengujian keamanan siber	Mengumpulkan informasi yang diperlukan untuk pengujian keamanan siber
			Mencari kerentanan sesuai ruang lingkup pengujian keamanan siber
		Memverifikasi keamanan siber	Menguji kerentanan pada objek pengujian
			Melakukan kegiatan setelah eksploitasi berdasarkan ruang lingkup pengujian keamanan siber
		Menyajikan laporan hasil pengujian keamanan siber	Melakukan kompilasi temuan hasil pengujian keamanan siber
			Menyusun laporan hasil pengujian keamanan siber

B. Daftar Unit Kompetensi

NO	Kode Unit	Judul Unit Kompetensi
1	*2*	*3*
1.	J.62UKS00.001.1	Merencanakan Prosedur Uji Keamanan Siber
2.	J.62UKS00.002.1	Menentukan Metode Penilaian Kerentanan
3.	J.62UKS00.003.1	Menentukan Ruang Lingkup Pengujian Keamanan Siber
4.	J.62UKS00.004.1	Menentukan Tim Penguji Keamanan Siber
5.	J.62UKS00.005.1	Mengumpulkan Informasi yang diperlukan untuk Pengujian Keamanan Siber
6.	J.62UKS00.006.1	Mencari Kerentanan Sesuai Ruang Lingkup Pengujian Keamanan Siber
7.	J.62UKS00.007.1	Menguji Kerentanan pada Objek Pengujian
8.	J.62UKS00.008.1	Melakukan Kegiatan Setelah Eksploitasi Berdasarkan Ruang Lingkup Pengujian Keamanan Siber
9.	J.62UKS00.009.1	Melakukan Kompilasi Temuan Hasil Pengujian Keamanan Siber
10.	J.62UKS00.010.1	Menyusun Laporan Hasil Pengujian Keamanan Siber

C. Uraian Unit Kompetensi

KODE UNIT : J.62UKS00.001.1

JUDUL UNIT : Merencanakan Prosedur Uji Keamanan Siber

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi kebutuhan informasi terkait perencanaan Uji Keamanan Siber (UKS) dalam rangka pembuatan prosedur pengujian keamanan siber sesuai ruang lingkup kebutuhan keamanan organisasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyiapkan kebutuhan informasi terkait perencanaan UKS	1.1 Aset Teknologi Informasi (Aset TI) diidentifikasi sebagai objek pengujian sesuai dengan ruang lingkup pengujian keamanan siber. 1.2 **Standar UKS** dipilih sesuai dengan proses bisnis dan ruang lingkup pengujian keamanan siber. 1.3 Strategi proses pengujian ditentukan berdasarkan kebutuhan pengujian.
2. Menyiapkan prosedur pengujian keamanan siber	2.1 Kerangka kerja pengujian menyeluruh ditetapkan pada setiap tahapan sesuai ruang lingkup pengujian keamanan siber. 2.2 Prosedur dan kewenangan pengujian dibuat berdasarkan ruang lingkup pengujian keamanan siber. 2.3 **Daftar perangkat untuk pengujian** keamanan siber dibuat sesuai ruang lingkup pengujian keamanan siber.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Standar UKS merupakan *framework* yang digunakan, antara lain *Payment Card Industry Data Security Standards* (PCI DSS) *Penetration Testing Guide*, *National Institute of Standards and Technology* (NIST) SP 800-115, *The Open Web Application Security*

Project (OWASP) Framework, The Penetration Testing Execution Standard (PTES), dan lain-lain.

1.2 Daftar perangkat untuk pengujian yang dimaksud seperti *scanner tools, proxy interception tools, exploit framework tools,* dan lain-lain yang akan digunakan dalam pengujian keamanan siber.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan pengolah kata
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*
      4.2.2 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik

yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan metode kombinasi demonstrasi/praktik simulasi, metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Standar pengujian keamanan siber

3.1.2 Manajemen Aset Teknologi Informasi (TI)

3.1.3 Manajemen risiko teknologi informasi

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah grafik presentasi

3.2.3 Merancang narasi untuk dapat membuat penjelasan yang mudah dipahami mengenai prosedur UKS

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mengidentifikasi Aset TI yang berkaitan dengan pengujian keamanan siber

4.2 Cara berpikir sistematis dan terstruktur dalam membuat prosedur pengujian keamanan siber

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi Aset TI sebagai objek pengujian sesuai dengan ruang lingkup pengujian keamanan siber

KODE UNIT : **J.62UKS00.002.1**

JUDUL UNIT : **Menentukan Metode Penilaian Kerentanan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menelaah dan mengidentifikasi metode penilaian kerentanan yang relevan terhadap hasil pengujian.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menelaah metode penilaian kerentanan yang relevan	1.1 Daftar metode dalam penilaian kerentanan disusun berdasarkan ruang lingkup pengujian keamanan siber. 1.2 Metode penilaian kerentanan yang tersusun dianalisis berdasarkan relevansi dengan ruang lingkup pengujian keamanan siber.
2. Mengidentifikasi metode penilaian kerentanan hasil Uji Keamanan Siber (UKS)	2.1 Bentuk **metriks dasar** untuk pengujian disiapkan berdasarkan hasil UKS. 2.2 **Komponen kerentanan** diperiksa berdasarkan pengujian keamanan siber. 2.3 Metode penilaian kerentanan dipilih berdasarkan relevansi terhadap hasil UKS.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Metrik dasar adalah metrik yang digunakan untuk penilaian tingkat kerentanan.
   1.2 Komponen kerentanan yang dimaksud berkaitan dengan komponen pada aset teknologi informasi yang memberikan dampak terhadap kerahasiaan, integritas, dan ketersediaan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan pengolah kata
      2.1.2 Peralatan yang terhubung ke jaringan

2.2 Perlengkapan

2.2.1 Kertas kerja ruang lingkup pengujian keamanan siber

2.2.2 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

4.2.2 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan metode kombinasi demonstrasi/praktik simulasi, metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Metode pengukuran *severity level* suatu Aset Teknologi Informasi (TI)
      3.1.2 Konsep eksploitasi, kemungkinan dan dampak kerentanan
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai metode penilaian kerentanan hasil pengujian keamanan siber

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam menentukan penilaian kerentanan
   4.2 Berpikir sistematis dan terstruktur dalam menelaah metode penilaian kerentanan yang relevan dengan hasil pengujian keamanan siber
   4.3 Bertanggung jawab terhadap pemilihan metode penilaian kerentanan

5. Aspek kritis
   5.1 Ketepatan dalam memilih metode penilaian kerentanan berdasarkan relevansi terhadap hasil UKS

KODE UNIT : **J.62UKS00.003.1**

JUDUL UNIT : **Menentukan Ruang Lingkup Pengujian Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi dan menetapkan ruang lingkup pengujian keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menganalisis ruang lingkup pengujian keamanan siber	1.1 **Objek pengujian** diidentifikasi berdasarkan Aset Teknologi Informasi (Aset TI). 1.2 Objek pengujian diidentifikasi berdasarkan **tingkat risiko** dalam organisasi. 1.3 Tujuan pengujian diidentifikasi berdasarkan kebutuhan organisasi. 1.4 Kerangka waktu diidentifikasi berdasarkan urgensi pengujian serta ketersediaan **sumber daya**.
2. Menetapkan ruang lingkup pengujian keamanan siber	2.1 Seluruh pemangku kepentingan yang berhubungan dengan kegiatan Uji Keamanan Siber (UKS) diidentifikasi sesuai kewenangannya. 2.2 Ruang lingkup pengujian ditentukan berdasarkan hasil analisis. 2.3 ***Rules of engagement*** dibuat berdasarkan **standar yang relevan**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Objek pengujian adalah sistem layanan, proses sistem layanan, infrastruktur, sistem internal, dan *embedded devices*.
   1.2 Tingkat risiko adalah skala risiko atas semua Aset TI yang ada dalam sebuah organisasi.
   1.3 Sumber daya yang dimaksud terdiri atas sumber daya manusia dan perangkat yang dibutuhkan dalam melaksanakan kegiatan pengujian keamanan siber.

1.4 *Rules of engagement* merupakan dokumen yang menjelaskan ketentuan larangan dan pembatasan dalam menjalankan UKS.

1.5 Standar yang relevan yang dimaksud merupakan standar/*framework*/regulasi pelaksanaan UKS yang memuat ketentuan terkait pembuatan *rules of engagement*.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Peralatan pengolah kata

2.1.2 Peralatan yang terhubung ke jaringan

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

4.2.2 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang

sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan metode kombinasi demonstrasi/praktik simulasi, metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Manajemen Aset TI

3.1.2 Manajemen risiko teknologi informasi

3.1.3 Standar dan prosedur UKS

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai ruang lingkup pengujian keamanan siber

4. Sikap kerja yang diperlukan

4.1 Tepat dalam pengambilan keputusan

4.2 Teliti dan cermat dalam menganalisis kebutuhan pengujian keamanan siber

4.3 Berpikir sistematis dan terstruktur dalam menentukan ruang lingkup pengujian keamanan siber

4.4 Bertanggung jawab dalam pembuatan *rules of engagement*

5. Aspek kritis

5.1 Ketepatan dalam menentukan ruang lingkup pengujian berdasarkan objek pengujian, tujuan pengujian, dan kerangka kerja pengujian keamanan siber

KODE UNIT : **J.62UKS00.004.1**

JUDUL UNIT : **Menentukan Tim Penguji Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi kebutuhan dan mengelola tim penguji dalam rangka menentukan tim penguji keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memeriksa kebutuhan tim penguji keamanan siber sesuai ruang lingkup pengujian keamanan siber	1.1 Kompetensi Sumber Daya Manusia (SDM) ditentukan sesuai ruang lingkup pengujian keamanan siber. 1.2 Beban kerja SDM diidentifikasi berdasarkan ruang lingkup pengujian keamanan siber. 1.3 Ketersediaan SDM diidentifikasi sesuai ruang lingkup pengujian keamanan siber.
2. Menyiapkan tim penguji keamanan siber	2.1 Tim penguji disusun berdasarkan hasil analisis kebutuhan. 2.2 **Manajemen tim** ditetapkan berdasarkan ruang lingkup pengujian keamanan siber.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Manajemen tim meliputi pembagian tugas pokok, fungsi, pemenuhan kerangka waktu pengujian keamanan siber, serta *monitoring* dan evaluasi kerja tim.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan yang terhubung ke jaringan
      2.1.2 Peralatan pengolah kata
   2.2 Perlengkapan
      2.2.1 Kertas kerja ruang lingkup pengujian keamanan siber
      2.2.2 Data ketersediaan SDM
      2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*
   4.2.2 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan, serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang memiliki laboratorium simulasi uji penetrasi.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.
   1.4 Hasil unjuk kerja yang berupa identifikasi mencakup kegiatan penuangan dan penyampaian hasil identifikasi menggunakan alat bantu untuk pengujian keamanan siber.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 *Project management*

3.1.2 Prosedur dan standar UKS

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai penyiapan tim penguji keamanan siber

4. Sikap kerja yang diperlukan

4.1 Kepemimpinan

4.2 Teliti dalam menelaah beban kerja tim penguji keamanan siber

4.3 Bertanggung jawab dalam mengelola tim penguji

4.4 Adil dalam membagi beban kerja tim penguji berdasarkan kompetensi dan kerangka waktu kerjanya

5. Aspek kritis

5.1 Ketepatan dalam menyusun tim penguji berdasarkan hasil analisis kebutuhan

KODE UNIT : **J.62UKS00.005.1**

JUDUL UNIT : **Mengumpulkan Informasi yang diperlukan untuk Pengujian Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menghimpun dan memeriksa informasi yang diperlukan sesuai ruang lingkup pengujian keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menghimpun informasi yang dianggap relevan	1.1 Kebutuhan **informasi yang relevan** diidentifikasi berdasarkan ruang lingkup pengujian keamanan siber. 1.2 Informasi yang relevan dikumpulkan berdasarkan ruang lingkup pengujian keamanan siber.
2. Memeriksa hasil penghimpunan informasi yang relevan	2.1 Informasi yang terhimpun dianalisis berdasarkan relevansinya terhadap ruang lingkup pengujian keamanan siber. 2.2 Hasil analisis dipetakan berdasarkan **tingkat reliabilitasnya** terhadap pelaksanaan Uji Keamanan Siber (UKS).

BATASAN VARIABEL

1. Konteks variabel
   1.1 Informasi yang relevan adalah semua jenis informasi yang dapat dipergunakan dalam pelaksanaan uji keamanan sesuai ruang lingkup pengujian keamanan siber, sebagai contoh informasi terkait mekanisme arsitektur sistem, *server*, sistem pencegahan, dan lain-lain.
   1.2 Tingkat reliabilitas adalah tingkat daya guna dari suatu informasi yang berhasil didapat dalam mendukung keberhasilan kegiatan UKS.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan yang terhubung ke jaringan

2.1.2 *Scanner tools, proxy interception tools, exploit framework tools*, dan lain-lain

2.2 Perlengkapan

2.2.1 Kertas kerja ruang lingkup pengujian keamanan siber

2.2.2 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Payment Card Industry Data Security Standard* (PCI DSS) *Penetration Testing Guide*

4.2.2 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

4.2.3 *The Open Web Application Security Project* (OWASP) *Framework*

4.2.4 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik

yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan cara demonstrasi/praktik simulasi yang dikombinasikan dengan metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Metode, teknik, dan prosedur UKS

3.1.2 Jaringan dan sistem operasi

3.1.3 *Open-Source Intelligence* (OSINT)

3.1.4 Pemetaan informasi

3.2 Keterampilan

3.2.1 Menggunakan aplikasi *scanning*

3.2.2 Mencari informasi dan data terkait kerentanan dan *exploit*

3.2.3 Mengolah data angka pada aplikasi *spreadsheet*

4. Sikap kerja yang diperlukan

4.1 Berpikir kritis dalam menghimpun informasi yang dianggap relevan

4.2 Teliti dalam menganalisis berbagai informasi yang dihimpun

4.3 Sistematis dan terstruktur dalam menelaah relevansi informasi yang dihimpun

4.4 Tepat dalam memetakan hasil pengumpulan informasi yang diperlukan

5. Aspek kritis

5.1 Ketepatan dalam memetakan hasil analisis berdasarkan tingkat reliabilitasnya terhadap pelaksanaan UKS

KODE UNIT : **J.62UKS00.006.1**

JUDUL UNIT : **Mencari Kerentanan Sesuai Ruang Lingkup Pengujian Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi dan memeriksa kerentanan pada objek pengujian yang ditemukan sesuai dengan ruang lingkup pengujian keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi kerentanan objek pengujian	1.1 Kerentanan pada objek pengujian dideteksi berdasarkan komparasi terhadap **basis data kerentanan**. 1.2 Daftar kerentanan disusun berdasarkan objek pengujian.
2. Memeriksa kerentanan objek pengujian	2.1 Daftar kerentanan dianalisis berdasarkan ***severity level*** terhadap objek pengujian. 2.2 Kerentanan yang bersifat ***false positive*** diidentifikasi berdasarkan hasil analisis daftar kerentanan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Basis data kerentanan adalah sekumpulan data yang merupakan referensi terkait kerentanan baik yang dipublikasikan maupun yang belum dan/atau tidak dipublikasikan.
   1.2 *Severity level* merupakan urutan tingkat penilaian risiko pada sistem elektronik berdasarkan hasil penilaian risiko. Umumnya bernilai: *critical, high, medium, low,* dan *information.*
   1.3 *False positive* merupakan suatu kondisi dimana kerentanan yang terdeteksi bukan merupakan suatu kerentanan setelah dilakukan pemeriksaan ulang.

2. Peralatan dan perlengkapan
   2.1 Peralatan

2.1.1 Peralatan yang terhubung ke jaringan

2.1.2 *Scanner tools, proxy interception tools, exploit framework tools*, dan lain-lain

2.2 Perlengkapan

2.2.1 Kertas kerja ruang lingkup pengujian keamanan siber

2.2.2 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Payment Card Industry Data Security Standard* (PCI DSS) *Penetration Testing Guide*

4.2.2 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

4.2.3 *The Open Web Application Security Project* (OWASP) *Framework*

4.2.4 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik

yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan cara demonstrasi/praktik simulasi yang dikombinasikan dengan metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Jaringan dan sistem

3.1.2 *Transmission Control Protocol/Internet Protocol* (TCP/IP) *concept & protocol*

3.1.3 *Scanning method*

3.1.4 Kerentanan dan *exploit*

3.1.5 Sistem operasi

3.2 Keterampilan

3.2.1 Menggunakan *scanner tools, proxy interception tools, exploit framework tools*, dan lain-lain

3.2.2 Mengolah data hasil pengujian keamanan siber

3.2.3 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai kerentanan yang ditemukan

4. Sikap kerja yang diperlukan

4.1 Kecermatan dalam menganalisis daftar kerentanan

4.2 Bertindak secara sistematis dan terstruktur dalam melakukan tahapan pengujian keamanan siber

4.3 Bertanggung jawab dalam menganalisis *severity level* objek pengujian

4.4 Teliti dalam menyusun daftar kerentanan berdasarkan objek pengujian

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi kerentanan yang bersifat *false positive* berdasarkan hasil analisis daftar kerentanan

KODE UNIT : **J.62UKS00.007.1**

JUDUL UNIT : **Menguji Kerentanan pada Objek Pengujian**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menguji kerentanan yaitu melalui identifikasi dan pemeriksaan parameter yang akan dieksploitasi pada objek pengujian.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan parameter yang akan dieksploitasi pada objek pengujian	1.1 ***Exploit*** yang relevan diidentifikasi untuk mengeksploitasi kerentanan berdasarkan objek pengujian. 1.2 *Exploit* atas **kerentanan tertentu** dibuat sesuai kebutuhan pengujian. 1.3 **Parameter yang akan dieksploitasi** ditentukan berdasarkan hasil analisis kerentanan dan ketersediaan *exploit* yang relevan.
2. Memeriksa parameter yang dieksploitasi pada objek pengujian	2.1 Eksploitasi parameter pada objek pengujian dilakukan dengan *exploit* yang dianggap relevan. 2.2 Hasil **eksploitasi** parameter pada objek pengujian dikompilasi berdasarkan **keberhasilan eksploitasi**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 *Exploit* adalah perangkat lunak atau sekumpulan perintah yang dapat digunakan untuk mengeksploitasi kerentanan pada objek pengujian. Contoh *exploit* misalnya, *EternalBlue* yang digunakan untuk eksploitasi *Server Message Block* (SMB) *vulnerability* pada sistem operasi *windows* (CVE-2017-0144).
   1.2 Kerentanan tertentu adalah *zero day vulnerability,* dan/atau kerentanan yang belum teridentifikasi.
   1.3 Parameter yang akan dieksploitasi adalah kerentanan pada objek pengujian yang akan dieksploitasi dengan menggunakan *exploit*.

1.4 Eksploitasi adalah kegiatan mendayagunakan *exploit* terhadap suatu kerentanan sehingga berhasil melakukan penetrasi ke dalam sebuah sistem. Eksploitasi tidak selalu penggunaan *exploit* terhadap objek pengujian. Contohnya dalam konteks *web application*, maka metode eksploitasi dapat berupa *injection* (*command injection* maupun *Structured Query Language* (SQL) *injection*), *Cross Site Scripting* (CSS); dalam konteks objek pengujiannya adalah manusia, maka yang dieksploitasi adalah psikologis manusia melalui metode *social engineering* dalam konteks infrastruktur, maka eksploitasi terhadap objek pengujian dapat menggunakan metode *Domain Name System* (DNS) *cache poisoning, Dynamic Host Control Protocol* (DHCP) *starvation, Wireless-Fidellity* (WiFi) *encryption attack, buffer overflow pada services, brute force login services, Virtual Local Access Network* (VLAN) *hopping* dan lain-lain.

1.5 Keberhasilan eksploitasi adalah kondisi dimana kerentanan pada objek pengujian berhasil dieksploitasi dengan menggunakan sebuah *exploit*. Agar eksploitasi berhasil dan dapat memenuhi ruang lingkup pengujian, maka hal-hal yang harus diperhatikan adalah:

1.5.1 Pencarian kerentanan atas objek pengujian tidak terbatas berdasarkan pada daftar kerentanan yang sudah ada, jika diperlukan penguji dapat secara terus menerus mencari kerentanan lain yang dapat dieksploitasi berdasarkan ruang lingkup pengujian.

1.5.2 Kegiatan eksploitasi dapat dilakukan pada berbagai parameter dan objek pengujian sepanjang masih dalam ruang lingkup pengujian.

1.5.3 Kegiatan eksploitasi dapat terus dilakukan sampai tujuan pengujian tercapai sesuai ruang lingkup pengujian.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Peralatan yang terhubung ke jaringan

2.1.2 *Scanner tools, proxy interception tools, exploit framework tools,* dan lain-lain

2.2 Perlengkapan

2.2.1 Kertas kerja ruang lingkup pengujian keamanan siber

2.2.2 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Payment Card Industry Data Security Standard* (PCI DSS) *Penetration Testing Guide*

4.2.2 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

4.2.3 *The Open Web Application Security Project* (OWASP) *Framework*

4.2.4 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik yang disediakan secara fisik maupun secara virtual dengan

menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan cara demonstrasi/praktik simulasi di *workshop*, lisan, tertulis di tempat kerja dan di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Prosedur dan standar Uji Keamanan Siber (UKS)

3.1.2 Manajemen risiko teknologi informasi

3.1.3 Metode UKS

3.2 Keterampilan

3.2.1 Menggunakan *scanner tools, proxy interception tools, exploit framework tools,* dan lain-lain

3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai hasil pengujian kerentanan

4. Sikap kerja yang diperlukan

4.1 Teliti dalam menganalisis daftar kerentanan pada objek pengujian

4.2 Bertindak secara sistematis dan terstruktur dalam melakukan tahapan pengujian keamanan siber

4.3 Bertanggung jawab terhadap hasil pengujian keamanan siber yang dilakukan berdasarkan ruang lingkup pengujian keamanan siber

5. Aspek kritis

5.1 Keberhasilan dalam melakukan eksploitasi parameter pada objek pengujian dengan *exploit* yang dianggap relevan

KODE UNIT : **J.62UKS00.008.1**

JUDUL UNIT : **Melakukan Kegiatan Setelah Eksploitasi Berdasarkan Ruang Lingkup Pengujian Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam meningkatkan hak akses, memastikan akses selalu dapat digunakan, melakukan *data exfiltration,* serta *covering track* pasca kegiatan eksploitasi berdasarkan ruang lingkup pengujian.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Meningkatkan hak akses	1.1 **Informasi yang relevan** diidentifikasi untuk meningkatkan hak akses berdasarkan ruang lingkup pengujian keamanan siber. 1.2 Peningkatan hak akses ditentukan berdasarkan hasil eksploitasi dan/atau penggunaan informasi yang relevan terhadap objek pengujian.
2. Memastikan akses selalu dapat digunakan	2.1 Informasi yang relevan untuk memastikan hak akses selalu dapat terjaga diidentifikasi berdasarkan ruang lingkup pengujian keamanan siber. 2.2 ***Backdoor*** dipasang berdasarkan ruang lingkup pengujian keamanan siber.
3. Melakukan aktivitas *data exfiltration*	3.1 Target ***data exfiltration*** diidentifikasi berdasarkan ruang lingkup pengujian keamanan siber. 3.2 Metode *data exfiltration* dianalisis sesuai dengan **kondisi objek pengujian.** 3.3 Hasil *data exfiltration* disimpan sesuai dengan *rules of engagement* yang disepakati oleh kedua belah pihak.
4. Melakukan *covering track*	4.1 **Data dan *file* objek pengujian** diidentifikasi berdasarkan kebutuhan kegiatan ***covering track***. 4.2 Data dan *file* yang relevan dihapus sesuai kebutuhan kegiatan *covering track.*

BATASAN VARIABEL

1. Konteks variabel
   1.1 Informasi yang relevan adalah informasi yang dibutuhkan untuk melakukan kegiatan meningkatkan dan menjaga hak akses yang meliputi kerentanan terkait dengan *privilege escalation*, data dari *database*, data *backup* konfigurasi, *routing table*, *path* untuk mengunggah *file*, dan lain-lain.
   1.2 *Backdoor* adalah perangkat lunak atau *script* yang digunakan untuk memperoleh akses pada sistem setelah terlebih dahulu mendapatkan *initial access* sebagai hasil kegiatan eksploitasi.
   1.3 Target *data exfiltration* adalah data yang menjadi tujuan pengujian berdasarkan ruang lingkup pengujian keamanan siber. Misalnya data *user id* dan *password*, data konfigurasi, data identitas pribadi, dan data lain yang dianggap perlu sesuai ruang lingkup pengujian keamanan siber.
   1.4 Kondisi objek pengujian adalah keadaan objek pengujian, baik dari sisi keamanan maupun infrastruktur yang akan mempengaruhi keberhasilan kegiatan *data exfiltration*.
   1.5 Data dan *file* objek pengujian adalah sekumpulan data dan file yang harus dihapus sebagai suatu bagian kegiatan yang berakibat terjadinya perubahan pada sistem, sehingga tujuan kegiatan *covering tracks* dapat terpenuhi. Misalnya file *backdoor*, *file logs*, data histori perintah, dan lain-lain.
   1.6 *Covering track* merupakan aktivitas penghapusan jejak digital dari data dan *file* objek pengujian agar tidak mengakibatkan terjadinya perubahan pada sistem setelah dilaksanakannya pengujian keamanan siber.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan yang terhubung ke jaringan
      2.1.2 *Scanner tools, proxy interception tools, exploit framework tools*, dan lain-lain

2.2 Perlengkapan

2.2.1 Kertas kerja ruang lingkup pengujian keamanan siber

2.2.2 Dokumen *rules of engagement*

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 *Payment Card Industry Data Security Standard* (PCI DSS) *Penetration Testing Guide*

4.2.2 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

4.2.3 *The Open Web Application Security Project* (OWASP) Framework

4.2.4 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan

pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan cara demonstrasi/praktik simulasi yang dikombinasikan dengan metode lisan atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Prosedur dan standar Uji Keamanan Siber (UKS)

3.1.2 Manajemen risiko teknologi informasi

3.1.3 Metode UKS

3.2 Keterampilan

3.2.1 Menggunakan *scanner tools*, *proxy interception tools*, *exploit framework tools*, dan lain-lain

3.2.2 Menggunakan aplikasi pengolah kata

3.2.3 Mengolah data angka pada aplikasi *spreadsheet*

3.2.4 Mengolah grafik presentasi

3.2.5 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai kegiatan setelah pengujian keamanan siber dilakukan

4. Sikap kerja yang diperlukan

4.1 Teliti dalam menelaah data yang terkait pengujian keamanan siber

4.2 Bertindak secara sistematis dan terstruktur dalam menentukan langkah-langkah yang diperlukan pasca kegiatan eksploitasi

4.3 Bertanggung jawab terhadap pengujian keamanan siber yang dilakukan

5. Aspek kritis

5.1 Ketepatan dalam menentukan peningkatan hak akses berdasarkan hasil eksploitasi dan/atau penggunaan informasi yang relevan terhadap objek pengujian

KODE UNIT : **J.62UKS00.009.1**

JUDUL UNIT : **Melakukan Kompilasi Temuan Hasil Pengujian Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi serta mendokumentasikan temuan hasil pengujian keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi temuan yang relevan	1.1 **Temuan** dikelompokkan berdasarkan ruang lingkup pengujian keamanan siber. 1.2 Temuan dianalisis relevansinya terhadap kebutuhan laporan berdasarkan ruang lingkup pengujian keamanan siber.
2. Mendokumentasikan temuan hasil pengujian keamanan siber	2.1 Temuan yang relevan diinventarisir berdasarkan kebutuhan laporan. 2.2 Temuan yang relevan disusun sesuai dengan format laporan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Temuan adalah semua data maupun informasi yang didapat sebagai hasil dari kegiatan pengujian berdasarkan ruang lingkup pengujian keamanan siber. Contohnya hasil *scanning* dari *tools scanner, screenshot* eksploitasi yang berhasil, *file* yang ditemukan ketika pengujian berlangsung, dan lain-lain.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan pengolah data
   2.2 Perlengkapan
      2.2.1 Dokumen acuan rekomendasi perbaikan
      2.2.2 Format laporan awal
      2.2.3 Format paparan

3. Peraturan yang diperlukan

   (Tidak ada.)

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*

   4.2.2 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

   1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

   1.4 Penilaian dapat dilakukan dengan metode kombinasi demonstrasi/praktik simulasi, dengan metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

   3.1 Pengetahuan

      3.1.1 *Hardening* celah kerentanan

      3.1.2 Teknik *optimizes and secure programming*

      3.1.3 Jaringan dasar dan lanjutan

   3.2 Keterampilan

      3.2.1 Menggunakan aplikasi pengolah kata

      3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

      3.2.3 Mengolah grafik presentasi

      3.2.4 Menyusun laporan sesuai format yang telah ditentukan

4. Sikap kerja yang diperlukan

   4.1 Teliti dalam mendokumentasikan seluruh temuan hasil pengujian keamanan siber

   4.2 Bertindak secara sistematis dan terstruktur dalam mengelompokkan temuan berdasarkan ruang lingkup pengujian keamanan siber

   4.3 Bertanggung jawab terhadap hasil pengujian keamanan siber

5. Aspek kritis

   5.1 Ketepatan dalam menganalisis relevansi temuan terhadap kebutuhan laporan berdasarkan ruang lingkup pengujian keamanan siber

KODE UNIT : **J.62UKS00.010.1**

JUDUL UNIT : **Menyusun Laporan Hasil Pengujian Keamanan Siber**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi dampak temuan terhadap organisasi dan merancang narasi laporan hasil pengujian keamanan siber.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi dampak temuan terhadap organisasi	1.1 Temuan dianalisis berdasarkan metode penilaian kerentanan. 1.2 Dampak temuan terhadap **organisasi** dikorelasikan berdasarkan tingkat keparahan dan penilaian risiko.
2. Membuat narasi laporan	2.1 **Narasi laporan** disusun berdasarkan dampak temuan sesuai dengan ruang lingkup pengujian keamanan siber. 2.2 **Ringkasan eksekutif** disusun sebagai pemaparan singkat untuk para pimpinan yang akan membaca laporan. 2.3 **Laporan** disusun secara lengkap berdasarkan ruang lingkup pengujian keamanan siber.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Organisasi adalah entitas berbadan hukum yang menjadi objek pengujian keamanan siber berdasarkan ruang lingkup pengujian. Contoh: kementerian/lembaga, perusahaan sebagai entitas bisnis, institusi pendidikan, rumah sakit, dan lain lain.
   1.2 Narasi laporan adalah uraian/penjelasan hasil pengujian keamanan siber yang disusun secara kronologis dengan memenuhi prinsip faktual, aktual, dan akurat secara deskriptif sesuai unsur-unsur *What, When, Where, Who, Why*, dan *How* (5W+1H).
   1.3 Ringkasan eksekutif adalah hasil kesimpulan singkat dari keseluruhan laporan hasil pengujian keamanan siber yang

disiapkan dalam rangka memberikan pemahaman dampak temuan kepada para pemangku kepentingan organisasi.

1.4 Laporan paling sedikit memuat ringkasan eksekutif dan laporan teknis yang isinya berupa rincian ruang lingkup pengujian, hasil pengumpulan informasi, dampak temuan, dan rekomendasi remidiasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Peralatan pengolah kata
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 *National Institute of Standards and Technology* (NIST) SP 800-115 *Technical Guide to Information Security Testing and Assessment*
      4.2.2 *The Penetration Testing Execution Standard* (PTES)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.2 Unit kompetensi ini harus diujikan secara konsisten pada seluruh elemen kompetensi dan dilaksanakan pada situasi pekerjaan yang

sebenarnya di tempat kerja atau di luar tempat kerja secara simulasi dilengkapi dengan peralatan kerja yang memadai baik yang disediakan secara fisik maupun secara virtual dengan menggunakan kombinasi metode uji untuk mengungkapkan pengetahuan keahlian dan sikap kerja sesuai dengan tuntunan standar.

1.3 Kondisi penilaian merupakan aspek dalam penilaian yang sangat berpengaruh atas tercapainya kompetensi ini terkait dengan melaksanakan pekerjaan pengujian keamanan siber.

1.4 Penilaian dapat dilakukan dengan metode kombinasi demonstrasi/praktik simulasi, metode lisan, atau tertulis di tempat kerja atau di Tempat Uji Kompetensi (TUK).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Standar Uji Keamanan Siber (UKS)

3.1.2 Manajemen Aset Teknologi Informasi (Aset TI)

3.1.3 Manajemen risiko teknologi informasi

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Menyusun narasi yang empiris dan mudah dipahami mengenai pengujian keamanan siber dalam laporan

4. Sikap kerja yang diperlukan

4.1 Teliti dalam menelaah temuan hasil pengujian keamanan siber

4.2 Teliti dalam menentukan korelasi antara temuan, tingkat keparahan, dan penilaian risiko

4.3 Bertanggung jawab terhadap laporan yang disusun

5. Aspek kritis

5.1 Ketepatan dalam menyusun laporan yang lengkap sesuai dengan ruang lingkup pengujian keamanan siber

BAB III
PENUTUP

Dengan ditetapkannya Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer, dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Uji Keamanan Siber, maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH