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;

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.62UKS00.009.1**

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