Poznámky k použitiu ukážkového testu

Tento ukážkový test je určený pre uchádzačov o certifikačnú skúšku z modulu **Bezpečnost pri využívaní IKT (IT Security, Sylabus V1.0).** Ukážkový test má dať uchádzačovi možnosť zoznámiť sa so štýlom a štruktúrou certifikačného testu. Neodzrkadľuje presne znenie ostrých certifikačných testov.
Tento test sa nesmie v žiadnom prípade použiť na ostré certifikačné testovanie.

Požiadavky na testovacie prostredie

Softvér

- MS Word 2007 alebo MS Word 2010
- Operačný systém Windows XP alebo Windows7
- Antivírusový program, v ktorom je možné plánovať antivírusovú kontrolu počítača a tiež vypnúť rezidentnú kontrolu. Ostré testy sú k dispozícii pre MS Security Essentials, ESET NOD32 (zapnutý rozšírený režim).
- Internetový prehliadač MS Internet Explorer alebo Mozilla Firefox
- Archivačný program, ktorý je schopný pracovať s heslovaním archívov ZIP (pozor Windows 7 to celkom nevie). Ostré testy sú k dispozícii pre 7-Zip.

Hardvér

- Schopnosť pripojiť sa k bezdrôtovej sieti. Netreba inštalovať špeciálnu sieť. Ukážkový test predpokladá len existenciu nejakých v okolí.
- Prístup k internetu
- Pri ostrých testoch nie je povolený ani potrebný prístup do siete Internet, stačí len zriadený WI-FI AP.

Súbor **modul 12_2014_B.zip** obsahuje ukážkový test. Súbor extrahujte archívnym programom napr. 7-Zip, WinRar, a pod. (ponúknuté nastavenia akceptujte archívneho programu).

Súbor **M12_Instrukcie a Zadanie_2014_B.pdf** obsahuje zadanie úloh alebo otázok, priečinok **M12_pracsub_2014_B** obsahuje príslušné pracovné súbory alebo prostredie.

Príprava pred testom: Na disk uchádzača treba umiestniť obsah priečinka **M12pracsub_2014_B**. Priečinok **odpovede** obsahuje súbor, kde sa ukladajú odpovede uchádzača.

Disk uchádzača fyzicky môže byť napríklad USB kľúč, samostatný disk alebo vyhradený priečinok na disku. Jednoznačná **Identifikácia uchádzača** je kódové číslo/ reťazec, používa sa v ostrých testoch.

Riešenia: Ak ste si nie istý so svojou odpoveďou a chceli by ste si potvrdiť správnosť, zašlite Kancelárii ECDL Slovenskej informatickej spoločnosti dotaz na adresu ecdl@ecdl.sk s príslušným číslom otázky a pride vám odpoveď.

Informácia o ostrých testoch

Ostré certifikačné testy obsahujú 23 teoretických otázok a 9 praktických úloh. Za správne riešenie každej otázky/ úlohy sa prideľuje 1 bod. Spolu 32 bodov. Na úspešné zvládnutie ukážkového testu treba minimálne 75% z plného počtu bodov (24 bodov).

Pri ostrej skúške má uchádzač o certifikát **zadanie úloh a otázok** vytlačené na papieri, nie v elektronickej forme. Formulácie otázok a úloh rešpektujú terminológiu softvérovej aplikácie, na ktorej sa skúška vykonáva. Otázky v teste je potrebné vykonávať v poradí, v akom sú predložené, pretože niektoré na seba nadväzujú. Uchádzač má pracovať len na svojom pridelenom „disku uchádzača“. Test musí byť ukončený do 45 minút. V prípade akéhokoľvek porušenia pravidiel sa test musí ukončiť.

Po teste je potrebné celú dokumentáciu a odpojiteľné pamäťové médiá odovzdať skúšobnému komisárovi. Žiadne súčasti nie je možné vyniesť.

Ref: ECDL / ICDL Module 12 - Syllabus – V1.0 - Sample Test - 2010 – V1 – 0

Ukážka testu M12b

Nasledujúci ukážkový test z **Modulu 12, *Bezpečnosť pri využívaní IKT*** obsahuje 11 teoretických a 7 praktických otázok. Ak je v otázke uvedených viac možných odpovedí, je správna IBA JEDNA z nich.

Teoretická časť

Na disku uchádzača v priečinku **odpovede** vyhľadajte dokument s názvom **Odpovede12b.doc** a otvorte ho. Svoje odpovede (a,b,c,d) zapisujte do tohto súboru a zmeny priebežne ukladajte.

B.1 Čo najlepšie opisuje termín **ethical hacking („etický prienik“)**?

a. Snaha primäť ľudí aby vykonali neautorizované úkony (akcie).

b. Snaha primäť ľudí aby prezradili dôvernú informáciu.

c. Ohrozenie dôverných údajov zo strany vlastných zamestnancov .

d. Autorizované testovanie, ktoré má zistiť bezpečnostné problémy.

B.2 Čo z nasledujúceho môže byť použité ako opatrenie na ochranu proti neautorizovanému prístupu k údajom?

a. Dešifrovanie dôverných súborov.

b. Šifrovanie dôverných súborov.

c. Inštalovanie malware.

d. Aktivovanie funkcie automatického dokončovania vo vašom webovom prehliadači (autocomplete feature).

B.3 Čo z nasledujúceho najlepšie opisuje parameter bezpečnosti informačného systému – **integritu**?

a. Vyžaduje autorizáciu na akúkoľvek modifikáciu údajov.

b. Vyžaduje iba jednu autorizáciu na zmeny údajov (len pri prvom prístupe do informačného systému).

c. Zabezpečuje, že údaje sú dostupné v ktoromkoľvek čase.

d. Potvrdzuje identitu všetkých zúčastnených strán (poskytovateľa aj záujemcu o údaje).

B.4 Čo z nasledujúceho najlepšie opisuje anglický termín **malware**?

a. Softvér, ktorého úlohou je dávať do karantény podozrivé súbory zo softvéru počítača.

b. Softvér, ktorého úlohou je spôsobovať zničenie dát alebo zníženie funkčnosti softvéru počítača alebo ohrozenie bezpečnosti údajov.

c. Softvér, ktorého úlohou je zaznamenávať všetku komunikáciu (na úrovni nadväzovania spojenia) a blokovať neautorizovaných odosielateľov.

d. Softvér, ktorého úlohou je urýchľovať časovo náročné a opakované úlohy.

Pokračovanie...

B.5 Čo z nasledujúceho vplýva na správnu funkčnosť antivírusového softvéru?

a. Deaktivuje sa, keď sa používateľ pripojí do siete LAN.

b. Vypnutý firewall.

c. Na zabezpečenie maximálnej ochrany je nutné pravidelne aktualizovať vírusovú databázu.

d. Vypnuté skenovanie (kontrolu) externých nosičov dát (napr. diskov, USB)

B.6 Čo z nasledujúceho sa používa na ochranu pred neautorizovaným (neoprávneným) prístupom do siete z vonkajších počítačových systémov ?

a. Rootkits.

b. Botnets („siete robotov“).

c. Programy typu Malware.

d. Firewall.

B.7 Čo z nasledujúceho sa považuje za dobrý návyk pri **online nákupoch**?

a. Používať funkciu automatického dokončovania, aby sa urýchlila transakcia (obchodná operácia).

b. Využívať techniku pharming, aby sa zabezpečila bezpečná transakcia.

c. Používať také webové sídla, ktoré vykonávajú transakcie cez zabezpečené stránky.

d. Používať také webové sídla, ktoré vyžadujú, aby boli povolené súbory cookies.

B.8 Čo z nasledujúceho je textová informácia, ktorú si uchováva váš webový prehliadač, keď navštívite nejakú webovú stránku?

a. Súbor cookie.

b. Definičný súbor (definition file).

c. Backdoor („zadné dvierka“)

d. Makro

B.9 Čo z nasledujúceho najlepšie opisuje účel **digitálneho podpisu**?

a. Verifikovanie identity odosielateľa e-mailu.

b. Vkladanie textového podpisu na spodok elektronického dokumentu pomocou spustenia makra.

c. Overuje, že e-mail bol doručený a nemal k nemu prístup žiadny neautorizovaný adresát

d. Je to šifrovací kľúč, ktorý sa používa na dešifrovanie e-mailu.

B.10 Akú **bezpečnostnú hrozbu** treba zvažovať pri otváraní prílohy elektronickej správy (e-mailu)?

a. Súbor môže obsahovať digitálny podpis.

b. Súbor pri otváraní vo vašom počítači môže zmazať vaše súbory cookies.

c. Pripojený súbor môže vyžadovať na prvé otvorenie zadanie hesla.

d. Pripojený súbor môže obsahovať makro.

Pokračovanie...

B.11 Čo z nasledujúceho NIE JE prostriedkom na trvalé vymazanie (zničenie) údajov?

a. Demagnetizácia (degaussing) nosiča dát, ktorý obsahuje súbory.

b. Vymazanie súborov z nosiča dát.

c. Rozdrvenie (shredding) pevného disku vášho počítača.

d. Opätovné naformátovanie nosiča dát, ktorý obsahuje príslušné údaje.

Praktická časť

B.12 Zistite počet pre vás viditeľných (dostupných, ak by ste mali prístupové údaje) bezdrôtových sietí. Zistený počet zapíšte do príslušného riadku v súbore **Odpovedeb12b.doc** a zmenu uložte

B.13 Spustite nainštalovaný internetový prehliadač. Prejdite na zabezpečenú webovú stránku https://www.ecdl.cz Zistite, kto vystavil certifikát, ktorým je stránka zabezpečená. Jeho názov zapíšte do príslušného riadku v súbore **Odpovede12b.doc** a zmeny v súbore uložte.

B.14 Otvorte súbor ***DHIM.xlsx*** na disku uchádzača. Na otvorenie použite heslo ***zajtra***. Uložte a zatvorte súbor ***DHIM***.

B.15 Pomocou archivačného programu extrahujte archív s názvom **Tlaciva-vzory*.zip*** z priečinka ***Zaloha skladu*** do priečinka ***Ostatne*** . Archív je zabezpečený heslom ***pondelok,*** ostatné ponúkané nastavenia akceptujte ***.***

B.16 Na disku uchádzača vyhľadajte súbor **Okres Brno-venkov.docx** a otvorte ho. Zistite, kto súbor digitálne podpísal a toto meno zapíšte do príslušného riadku v súbore **Odpovede12b.doc** a zmeny v súbore uložte

B.17 Otvorte používateľské rozhranie antivírusového programu a naplánujte antivírusovú kontrolu počítača tak, aby prebiehala **každý deň o 23.00 večer** (ak program požaduje názov úlohy, nazvite ju: UCH; ostatné nastavenia plánovanej úlohy akceptujte).

Na záver tlačidlo „Ukončiť“ NESTLAČTE, ale aktuálne okno (stlačte Alt+PrtScn) skopírujte (vložiť) do súboru **Odpovede12b.doc**. Plánovanú úlohu Zrušte.

Poznámka: Úloha predpokladá, že počítač máte o takomto čase vždy zapnutý.

B.18 Vo vašom internetovom prehliadači odstráňte IBA **dočasne uložené súbory**.

Uložte a uzatvorte všetky otvorené súbory a aplikácie.

KONIEC UKÁŽKY TESTU M12b