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_A.zip** obsahuje ukážkový test. Súbor extrahujte archívnym programom (ponúknuté nastavenia akceptujte archívneho programu).

Súbor **M12_Instrukcie a Zadanie_2014_A.pdf** obsahuje zadanie úloh alebo otázok, priečinok **M12pracsub_2014_A** obsahuje príslušné pracovné súbory alebo prostredie.

Príprava pred testom: Na disk uchádzača treba umiestniť obsah priečinka **M12pracsub_2014_A**. 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 M12a

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 **Odpovede12a.doc** a otvorte ho. Svoje odpovede (a,b,c,d) zapisujte do tohto súboru a zmeny priebežne ukladajte.

A.1 Čo z nasledujúceho je súčasťou **kyberzločinu**?

a. Decrytpion („dešifrovanie“).

b. Phishing („lov hesiel“).

c. Vyššia moc.

d. Ethical hacking („etický prienik“).

A.2 Čo z nasledujúceho najlepšie opisuje termín **červ**?

a. Vírus, ktorý sa sám kopíruje a nevyžaduje podnet od človeka.

b. Backdoor („zadné dvierka“) do operačného systému , ktoré dovolia neoprávneným používateľom prístup do siete.

c. Typ vírusu, ktorý sa maskuje ako užitočný softvér, ale len čo sa nainštaluje zničí počítač.

d. Typ vírusu, ktorý sa nerozmnožuje.

A.3 Čo z nasledujúceho najlepšie opisuje činnosť nazývanú **pharming**?

a. Presmerovanie používateľov na falošnú webovú stránku bez ich vedomia.

b. Zisťovanie bezpečnostných problémov v operačnom systéme cez autorizované testovanie operačného systému.

c. Získavanie osobných informácií od ľudí pomocou nevyžiadaných telefonických hovorov.

d. Zber informácií o používateľovi na základe jeho návykov pri prehľadávaní webových stránok, bez jeho vedomia.

A.4 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).

Pokračovanie...

A.5 Čo z nasledujúceho možno považovať za priamy dôsledok aktivity, ktorá patrí do **sociálneho inžinierstva**?

a. Vznikol problém s dostatkom voľnej pamäte.

b. Zriadila sa možnosť neoprávneného prístupu do počítača.

c. Vylepšil sa bezpečnostný parameter - integrita údajov.

d. Vylepšil sa bezpečnostný parameter - dostupnosť údajov.

A.6 Čo z nasledujúceho najlepšie opisuje anglický termín **botnet („sieť robotov“)**?

a. Typ softvéru, ktorý bol stiahnutý nelegálne bez zakúpenia licencie.

b. Skupina počítačov, ktoré boli nastavené tak, aby zaznamenávali telefónne čísla, ktoré boli volené (vytáčané).

c. Typ softvéru, ktorého úlohou je blokovať nelegálnu alebo neželanú komunikáciu.

d. Skupina počítačov, ktoré boli nastavené tak, aby posielali ďalej prebiehajúce prenosy bez súhlasu ich majiteľa(ov).

A.7 Čo z nasledujúceho označuje typ siete, ktorá poskytuje vzdialeným používateľom bezpečný vzdialený prístup do siete ich zamestnávateľa?

a. VPN

b. WI-FI

c. MAC

d. LAN

A.8 Čo z nasledujúceho je príklad **biometrickej techniky**, ktorá sa využíva na riadenie prístupu?

a. Skenovanie očí.

b. Pretexting („predstieranie situácie“)

c. Firewall.

d. Heslo.

A.9 Čo z nasledujúceho je jedným zo znakov, že webová stránka je zabezpečená?

a. .org

b. .edu

c. https

d. www

A.10 Čo z nasledovného najlepšie opisuje cieľ **šifrovania** elektronických správ (e-mailov)?

a. Používa sa na overenie, že e-mail neobsahuje škodlivý softvér.

b. Používa sa na zabezpečenie, aby správu mohla čítať len osoba, ktorej bola určená.

c. Používa sa v technike phishing, ktorá zabezpečuje distribuovanie elektronickej správy veľkej skupine adresátov.

d. Používa sa na zaistenie, aby e-mail, ktorý obsahuje makro neobsahoval vírusy.

Pokračovanie...

A.11	Ako sa označuje v elektronickom svete nelegálna činnosť, ktorej cieľom je uviesť osobu **do omylu o identite pôvodcu správy**, aby bolo možné získať cenné informácie? a. Ethical hacking („etický prienik“). b. Pretexting („predstieranie situácie“). c. Cracking („prelamovanie ochrany“) d. Phishing (“lov hesiel”).

Praktická časť

A.12	Zistite počet pre vás viditeľných (dostupných, ak by ste mali prístupové údaje) bezdrôtových sietí. Zistený počet zapíšte do príslušného riadku v súbore **Odpovede 12a.doc** a zmenu uložte
A.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 **Odpovede12a.doc** a zmeny v súbore uložte.
A.14	Otvorte súbor ***DHIM.xlsx*** na disku uchádzača. Na otvorenie použite heslo ***zajtra***. Uložte a zatvorte súbor ***DHIM***.
A.15	V priečinku ***Ostatne*** skomprimujte pomocou archivačného programu (napr. 7-Zip) všetky súbory Excelu do archívu s názvom ***Financie.zip*** a archív zabezpečte heslom ***Heslo@2***
A.16	Pomocou bežných prostriedkov Prieskumníka (kopírovať, vložiť) vytvorte na disku uchádzača v adresári ***Zaloha skladu*** zálohu archívu **Financie.zip**.
A.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 **Odpovede12a.doc**. Plánovanú úlohu Zrušte. Poznámka: Úloha predpokladá, že počítač máte o takomto čase vždy zapnutý.
A.18	Vo vašom internetovom prehliadači odstráňte IBA **históriu navštívených stránok**.

Uložte a uzatvorte všetky otvorené súbory a aplikácie.

KONIEC UKÁŽKY TESTU M12a

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