Poznámky k oficiálním cvičným testům pro modul M12

Testovací platforma

- Software
  - MS Word 2007 až 2010.
  - Operační systém Windows (XP, 7)
  - Antivirový program, v němž je možno provést test jedné konkrétní složky a v němž je možno plánovat testy. Ostré QTB jsou nyní k dispozici pro AVG, AVAST, ESET.
  - Internetový prohlížeč MS Internet Explorer, Mozilla Firefox, Google Chrome.
  - Archivační program, který je schopen pracovat s heslováním archivů ZIP (pozor, Windows 7 to zcela neumí). Ostré QTB jsou nyní k dispozici pro 7zip.
- Hardware
  - Schopnost připojení k bezdrátové síti. Speciální síť není třeba instalovat. Cvičné testy předpokládají pouze „nějaké sítě kolem".
  - Podle aktuální situace je třeba upřesnit zadání úkolu 11. Pokud komunikace s bezdrátovými sítěmi k dispozici není, stačí úkol 11 zrušit.
- Přístup k Internetu
  - V úkolu 12 se pracuje se zabezpečenou internetovou stránkou. Aby se stránka nemusela komplikovaně připravovat na lokálních počítačích (jako při ostrém testu), je připravena na webu ECDL.
  - Přístup k Internetu bude mít „negativní důsledek" možnost zjistit odpovědi na teoretické otázky na internetu. (Jde o cvičný test – záleží na „odpovědnosti" účastníka.)

Vyhodnocení cvičného testu

- Cvičné testy pro modul M12 nejsou připraveny tak, aby je bylo možno kompletně vyhodnotit „off line" jako testy ostré. U některých praktických úkolů chybí ověřování splnění (které je v ostrém testu řešeno snímáním screenshotů a jejich přenášením do souboru Odpovědi). V obou cvičných variantách jde o úkoly 14 až 16.
- Pokud je třeba seznámit uchazeče se správným řešením, pak je vhodné provést to „veřejně" po skončení cvičného testu.

Trénink 12a – Word 2007-2010

Spusťte textový editor a otevřete dokument ***Odpovědi.rtf*** ze složky ***Trenink M12.*** Odpovědi na teoretické otázky 1 až 10 zapisujte do tabulky v souboru ***Odpovědi.rtf***

1.

Jak nazýváme zabezpečený vzdálený přístup ke vzdálené počítačové síti (např. přístup k síti zaměstnavatele z domácího pracoviště)?

a) Backdoor (zadní vrátka).
b) VPN (virtuální privátní síť).
c) Ethical hacking (etický hacking).
d) FTP (file transfer protocol).

2.

Které z následujících hesel nejlépe splňuje pravidla pro tvorbu bezpečných hesel?

a) frantab
b) Franta_B
c) Frant@35#FB
d) 12.3.1987

3.

K čemu jsou využívány (nebo zneužívány) v oblasti počítačové bezpečnosti tzv. ***biometrické techniky?***

a) K nelegálnímu získávání DNA.
b) K nenávratné likvidaci dat.
c) K šifrování dat.
d) K ověření identity uživatele.

4.

Který z následujících pojmů může představovat přímé nebezpečí pro vaše nezletilé dítě?

a) Kybernetická šikana.
b) Firewall.
c) Komprese souborů se školními úlohami.
d) Neaktualizovaný internetový prohlížeč.

5.

Jaký rozdíl (nebo jaký vztah) je mezi pojmy ***digitální podpis*** a ***digitální certifikát?***

a) Pomocí digitálního podpisu lze k dokumentu připojit digitální certifikát.
b) Pomocí digitálního certifikátu lze k dokumentu připojit digitální podpis.
c) Digitální podpis lze zakoupit u certifikační autority, digitální certifikát nikoliv.
d) Digitální podpis a digitální certifikát jsou pouze dvě různá označení neprosto stejného pojmu.

6.

Co znamená zkratka ***WAN?***

a) Virtuální počítačovou síť.
b) Místní počítačovou síť (např. pro firmu sídlící v jedné budově).
c) Rozsáhlou počítačovou síť.
d) Pracovní počítačovou síť, v níž se pracuje pouze s dočasnými soubory.

7.

K čemu slouží ***demagnetizace*** pevného disku?

a) K odstranění škodlivého softwaru.
b) K trvalému odstranění dat.
c) K prodloužení trvanlivosti uložení dat.
d) K šifrování dat.

8.

Co je cílem techniky sociálního inženýrství nazývané ***phishing?***

a) Šikanování napadené osoby prostřednictvím Internetu.
b) Zpomalení práce internetového prohlížeče napadené osoby.
c) Získávání osobních nebo přihlašovacích údajů napadené osoby pomocí falešných emailů.
d) Zasílání nevyžádaných obchodních sdělení napadené osobě.

9.

Co jsou soubory ***cookies?***

a) Vždy jde o škodlivý software.
b) Jde o digitální certifikáty navštívených zabezpečených webových stránek.
c) Jde o aktualizované soubory virové databáze.
d) Jde o soubory, které ukládá internetový server do počítače uživatele.

10.

Do jaké kategorie můžeme zařadit oblíbené prostředky ***ICQ*** nebo ***Skype***?

a) Elektronická pošta.
b) Instant messaging (komunikace v reálném čase).
c) Sociální sítě.
d) Telegraf.

Úkoly 11 – 13 jsou praktické, avšak výsledky budete opět přenášet do souboru ***Odpovědi.rtf***.

11.

Zjistěte počet dostupných bezdrátových sítí, jejichž název začíná …… . Zjištěný počet zapište do souboru ***Odpovědi.rtf.***

12.

Do souboru ***Odpovědi.rtf*** krátce popište postup, jak připojit k dokumentu ve formátu ***DOCX*** digitální podpis (předpokládejte, že potřebný osobní certifikát je umístěn v centrálním úložišti certifikátu operačního systému Windows).

13.

Spusťte internetový prohlížeč. Přejděte na zabezpečenou webovou stránku ***https://www.ecdl.cz*** Zjistěte, kdo vystavil certifikát, kterým je stránka zabezpečena. Název vystavitele certifikátu zapište do souboru ***Odpovědi.rtf*** .

Zbývající úkoly 14 – 20 už jsou pouze praktické, soubor ***Odpovědi.rtf*** můžete uložit a zavřít.

14.

Otevřete uživatelské rozhraní vašeho antivirového programu a proveďte naplánování antivirového testu tak, aby proběhl ***každý den*** ve ***23:00*** večer (ostatní nastavení naplánované úlohy zvolte).

15.

Ve vašem internetovém prohlížeči proveďte odstranění POUZE ***historie navštívených stránek.***

16.

Změňte nastavení vašeho internetového prohlížeče tak, aby byly zcela vypnuty všechny ***funkce automatického dokončování*** (adresy, formuláře, uživatelská jména a hesla).

17.

Ve složce ***Trenink M12*** budete pracovat se soubory podsložek ***Objednávky*** a ***Archivace.*** Pomocí běžných prostředků operačního systému (program Průzkumník) obnovte zálohu POUZE archivu ***Stížnosti 2010.zip*** z podsložky ***Archivace*** do podsložky ***Objednávky.***

18.

Archiv z minulého úkolu ***Stížnosti 2010.zip*** extrahujte pomocí archivačního programu do podsložky ***Objednávky*** (archiv je zabezpečen heslem ***LuckaXXL>110-110-110***).

19.

Pomocí běžných prostředků operačního systému (program Průzkumník) vytvořte zálohu POUZE všech souborů změněných ***v roce 2011*** z podsložky ***Objednávky*** do podsložky ***Archivace.***

20.

Ve složce ***Trenink M12*** vyhledejte soubor ***Osobní údaje.docx*** . Soubor otevřete a zabezpečte jej heslem ***J23-&-kopyto*** tak, aby bez znalosti tohoto hesla nebylo možné soubor otevřít.

Uložte všechny otevřené dokumenty a uzavřete všechny programy.

Trenink 12b – Word 2007-2010

Spusťte textový editor a otevřete dokument ***Odpovědi.rtf*** ze složky ***Trenink M12.*** Odpovědi na teoretické otázky 1 až 4 zapisujte do tabulky v souboru ***Odpovědi.rtf***

1.

Jak nejlépe zajistíme data před neoprávněným přístupem jiné osoby?

a) Používáním pravidelně aktualizovaného antivirového programu.
b) Používáním elektronického podpisu.
c) Šifrováním dat.
d) Zamezením spouštění maker.

2.

Která z následujících technik má nejčastěji za cíl krádež identity napadené osoby?

a) Zasílání podvržených emailů.
b) Blokování cookies.
c) Pravidelná aktualizace virové databáze antivirového programu.
d) Fyzická likvidace pevných disků.

3.

Jak můžeme souhrnně pojmenovat škodlivé programy, které se nainstalují do počítače bez vědomí nebo souhlasu uživatele?

a) Antivirové programy.
b) Digitální certifikáty.
c) Malware.
d) Operační systémy.

4.

Co je vhodné (mimo jiné) udělat před připojením počítače do neznámé nezabezpečené bezdrátové sítě?

a) Instalovat osobní digitální certifikát.
b) Vypnout firewall.
c) Zapnout sdílení souborů.
d) Vypnout sdílení souborů.

5.

Jak prověříme pravost navštívené internetové stránky?

a) Podle URL adresy (musí začínat http://…)
b) Podle kontaktních údajů (adresa firmy, jméno kontaktní osoby atd.) uvedených na stránce.
c) Ověřením certifikátu, kterým je stránka zabezpečena.
d) Pomocí rezidentního štítu antivirového programu.

6.

Je (z hlediska bezpečnosti) vhodné zveřejnit na sociální síti svoji adresu?

a) Ano, zveřejnění adresy nepředstavuje riziko.
b) Raději ne.
c) Ano, ale pouze pro osoby starší 18 let.
d) Ano, ale pouze na sociální síti Facebook.

7.

Která z těchto ***biometrických technik*** se používá pro kontrolu identity uživatele?

a) Odběr DNA.
b) Skenování oka.
c) Záznam hlasu.
d) Odběr krve.

8.

Jak nejlépe ochráníme data před účinky tzv. ***„vyšší moci"?***

a) Zálohováním dat a ukládáním záloh na různých místech.
b) Šifrováním dat.
c) Pravidelnou demagnetizací pevných disků.
d) Kompresí dat.

9.

Co je ***shoulder surfing?***

a) Odezírání zadávaných informací z monitoru počítače „přes rameno".
b) Prohlížení internetových stránek pod cizím uživatelským jménem.
c) Prolamování hesel.
d) Komunikace dvou nebo více osob prostřednictvím internetu v reálném čase.

10.

Jak trvale odstraníme data z pevného disku počítače?

a) Odstraněním souboru do koše operačního systému Windows.
b) Odstraněním souboru do koše operačního systému Windows a následným „vysypáním" koše.
c) Zašifrováním dat.
d) Vícenásobným přepisem dat na pevném disku.

Úkoly 11 – 13 jsou praktické, avšak výsledky budete opět přenášet do souboru ***Odpovědi.rtf*** .

11.

Zjistěte typ zabezpečení bezdrátové sítě …… . Typ zabezpečení zapište do souboru ***Odpovědi.rtf***.

12.

Ve složce ***Trenink M12*** vyhledejte soubor ***Okres Brno-venkov.docx*** a otevřete jej. Zjistěte, kdo soubor digitálně podepsal a toto jméno zapište do souboru ***Odpovědi.rtf.***

13.

Spusťte internetový prohlížeč. Přejděte na zabezpečenou webovou stránku ***https://www.ecdl.cz*** Zjistěte, datum začátku platnosti certifikátu, kterým je stránka zabezpečena. Datum zapište do souboru ***Odpovědi.rtf***.

Zbývající úkoly 14 – 20 už jsou pouze praktické, soubor ***Odpovědi.rtf*** můžete uložit a zavřít.

14.

Pomocí vašeho antivirového programu proveďte antivirový test POUZE ve složce ***Různé*** (je podsložkou složky ***Trenink M12***).

15.

Ve vašem internetovém prohlížeči proveďte odstranění POUZE ***dočasně uložených souborů.***

16.

Změňte nastavení vašeho internetového prohlížeče tak, aby došlo k ***zablokování ukládání všech souborů cookies*** do počítače.

17.

Ve složce ***Trenink M12*** budete pracovat se soubory podsložek ***Objednávky*** a ***Archivace.*** Pomocí běžných prostředků operačního systému (program Průzkumník) obnovte zálohu POUZE souboru ***Masna Tlouštík a synové.xlsx*** z podsložky ***Archivace*** do podsložky ***Objednávky.***

18.

V podsložce ***Objednávky*** zkomprimujte pomocí archivačního programu POUZE všechny prezentace PowerPointu do archivu s názvem ***Prezentace.zip*** archiv zabezpečte heslem ***Heslo#2***

19.

Pomocí běžných prostředků operačního systému (program Průzkumník) vytvořte zálohu POUZE archivu z minulého úkolu ***Prezentace.zip*** z podsložky ***Objednávky*** do podsložky ***Archivace.***

20.

Ve složce ***Trenink M12*** vyhledejte soubor ***Dotazník.docx*** . Soubor otevřete (soubor je zabezpečen heslem ***5@-PIC-bum***). Dotazník vyplňte (zvolte libovolné odpovědi), změny v souboru uložte a soubor ***Dotazník.docx*** uzavřete.

Uložte všechny otevřené dokumenty a uzavřete všechny programy.