Poznámky k cvičnému testu M12

Software

- antivirový program, v němž je možno provést test jedné konkrétní složky a v němž je možno plánovat testy
- textový editor Microsoft Word (2007 a vyšší)
- obvyklý webový prohlížeč (Microsoft Edge, Mozilla Firefox, Google Chrome, příp. další (napřed ověřit schopnost splnit praktické úkoly)
- archivační program 7ZIP
- operační systém Windows (7 a vyšší)

Hardware, přístup k internetu

- možnost a schopnost připojení k bezdrátové síti
  - speciální síť není třeba instalovat, cvičný test předpokládá pouze „nějaké sítě kolem"
- podle aktuální situace je třeba upřesnit zadání úkolu 11

Vyhodnocení cvičného testu

- U cvičného testu se nepředpokládá „off line" hodnocení. Některé úkoly nezanechávají digitální stopu.
- Pro ověření postupů studentů je tedy vhodná demonstrace řešení.

Trenink M12a

Spusťte textový editor a otevřete dokument ***Odpovědi.rtf*** ze složky ***Trenink M12a.*** 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.

K čemu lze využít ***osobní hotspot?***

a) K bezpečnému rozpoznávání pharmingu.
b) K poskytnutí internetového připojení chytrého mobilního telefonu jinému mobilnímu zařízení.
c) Ke kompresi souborů.
d) K zabezpečení bezdrátové sítě.

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.

Zjistěte, zda je na vašem počítači momentálně zapnuta brána Firewall. Odpověď (Ano / Ne) zapište do souboru ***Odpovědi.rtf.***

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 M12a*** 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 M12a*** 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 M12b

Spusťte textový editor a otevřete dokument ***Odpovědi.rtf*** ze složky ***Trenink M12b.*** 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?

a) Zasílání podvržených emailů.
b) Blokování cookies.
c) Grooming.
d) Shredding.

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"*** jako jsou požár, povodeň apod.?

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) Použitím speciálního programu pro trvalé odstranění dat.

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 M12b*** vyhledejte soubor ***Hory.jpg*** Otevřete okno, ve kterém byste provedli zašifrování tohoto souboru (zašifrování NEPROVÁDĚJTE). Vytvořte snímek obrazovky a vložte jej 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 M12b***).

15.

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

16.

Zařiďte, aby s vaším počítačem nebylo možno komunikovat z jiného počítače pomocí programu ***Vzdálená plocha.***

17.

Ve složce ***Trenink M12b*** 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 M12b*** 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.