Primer testa za Modul 7 – IT sigurnost

1.1 Šta je od navedenog primer sajber kriminala? **[1 Bod]**

a. Dešifrovanje (decryption). ☐
b. Pecanje (Phishing) ☐
c. Viša sila. ☐
d. Etičko hakovanje. ☐

1.2 Šta od navedenog najbolje opisuje termin Etičko hakovanje? **[1 Bod]**

a. Skupljanje ljudi da izvrše neovlašćene radnje. ☐
b. Skupljanje ljudi da otkriju poverljive informacije. ☐
c. Pretnja poverljivim podacima od strane internog osoblja. ☐
d. Ovlašćeno testiranje za utvrđivanje eventualnih sigurnosnih sistemskih problema. ☐

1.3 Šta od navedenog najbolje opisuje čin pharming-a? **[1 Bod]**

a. Preusmerenje korisnika na lažni veb sajt bez njihovog znanja. ☐
b. Utvrđivanje eventualnih sistemskih problema ovlašćenim testiranjem. ☐
c. Skupljanje ličnih informacija ljudi putem telefonskih poziva. ☐
d. Prikupljanje informacija navika korisnika putem veb čitača, bez njihovog znanja. ☐

1.4 Šta od navedenog najbolje opisuje integritet kod informacione bezbednosti? **[1 Bod]**

a. Integritet zahteva autorizaciju za svaku promenu podataka. ☐
b. Integritet obezbeđuje zaštitu podataka od neovlašćenog pristupa. ☐
c. Integritet osigurava da su podaci uvek dostupni. ☐
d. Integritet potvrđuje identitet svih strana. ☐

1.5 Šta se od navedenog može koristiti za prikrivanje zlonamernog programa? **[1 Bod]**

a. Fajlovi bez makro naredbi. ☐
b. Razmagnetisani (degaussed) fajlovi. ☐
c. Rootkits. ☐
d. Zaštitni zid (firewall). ☐

1.6 Šta je od navedenog mana anti-virus programa? **[1 Bod]**

a. Program se deaktivira kada je korisnik konektovan na LAN. ☐
b. Program zahteva aktivaciju od zaštitnog zida. ☐
c. Program zahteva redovno ažuriranje za maksimalnu zaštitu. ☐
d. Program se ne može koristiti za skeniranje spoljnih uređaja. ☐

1.7 Šta se od navedenog koristi za sprečavanje neovlašćenog pristupa mreži? **[1 Bod]**

a. Rootkits. ☐
b. Botnets. ☐
c. Zlonamerni program. ☐
d. Zaštitni zid. ☐

1.8 Koja od navedenih ikona predsta konekciju putem mrežnog kabla? **[1 Bod]**

a.  ☐
b.  ☐
c.  ☐
d.  ☐

1.9 Šta od navedenog predstvlja bezbedan veb sajt? **[1 Bod]**

a. .org ☐
b. .edu ☐
c. https ☐
d. www ☐

1.10 Šta od navedenog skladišti veb čitač kao tekstualnu informaciju nakon posete veb sajtu? **[1 Bod]**

a. Kolačić (cookie). ☐
b. Definicijski fajl. ☐
c. „Stražnja vrata“ (back door). ☐
d. Makro naredba. ☐

1.11 Koje od navedenih podešavanja NE MOŽETE izmeniti na sajtu društvene mreže? **[1 Bod]**

a. Informacije o navikama i hobijima. ☐
b. Činjenicu da ste podesili nalog. ☐
c. Kontrolu privatnosti koje ste podesili. ☐
d. Lične detalje i kontakte. ☐

1.12 Šta od navedenog najbolje opisuje svrhu šifrovanja e-mail poruke? **[1 Bod]**

a. Potvrda da e-mail poruka ne sadrži zlonamerni program. ☐
b. Potvrda da je e-mail poruku pročitao samo onaj kome je namenjena. ☐
c. Šifrovanje se koristi za „pecanje“ kako bi e-mail poruka bila prosleđena velikom broju ljudi. ☐
d. Šifrovanje se koristi kako bi bili sigurni da e-mail poruke sa makro naredbama ne sadrže viruse. ☐

1.13 Šta od navedenog može biti pretnja za sigurnost pri otvaranju e-mail priloga? **[1 Bod]**

a. Fajl koji sadrži digitalni potpis. ☐
b. Fajl koji može da obriše kolačiće (cookies) po otvaranju poruke. ☐
c. Fajl koji zahteva jednokratnu šifru. ☐
d. Fajl koji sadrži makro naredbe. ☐

1.14 Šta se od navedenog može biti pretnja kod instant poruka? **[1 Bod]**

a. Biometrijski identitet. ☐
b. Etičko hakovanje. ☐
c. Stražni pristup (backdoor access). ☐
d. Pristup u realnom vremenu. ☐

1.15 Šta od navedenog NIJE trajno uništavanje podataka? **[1 Bod]**

a. Razmagnetisanje diska koji sadrži fajlove. ☐
b. Brisanje fajlova sa diska. ☐
c. „Seckanje“ (shredding) hard diska. ☐
d. Reformatiranje diska koji sadrži podatke. ☐

Sačuvajte i zatvorite fajl ***IT sigurnost primer testova - Teorijska pitanja 1*** i nastavite sa rešavanjem praktičnog testa od pitanja broj 2.