





Sample Test - Teoria

- 1.1 Quale dei seguenti è un tipo di crimine informatico? **[1 punto]**
- a. Decrittazione ☐
 - b. Phishing ☐
 - c. Forza maggiore ☐
 - d. Hacking etico ☐
- 1.2 Quale delle seguenti è una definizione del termine "hacking etico"? **[1 punto]**
- a. Far eseguire azioni non autorizzate alle persone. ☐
 - b. Far divulgare informazioni confidenziali alle persone. ☐
 - c. Una minaccia per i dati riservati da parte di personale interno ad un'azienda. ☐
 - d. Test autorizzati per determinare quali sono i problemi di sicurezza di un sistema. ☐
- 1.3 Quale delle seguenti descrizioni si riferisce all'attività di "pharming"? **[1 punto]**
- a. Ridirigere gli utenti verso un sito web falso senza che se ne accorgano. ☐
 - b. Determinare i problemi di sicurezza di un sistema attraverso dei test autorizzati. ☐
 - c. Raccogliere informazioni personali dalle persone attraverso telefonate non richieste. ☐
 - d. Raccogliere informazioni sulle abitudini di navigazione internet degli utenti senza il loro consenso. ☐
- 1.4 Quale delle seguenti caratteristiche descrive la caratteristica IT dell'integrità? **[1 punto]**
- a. Richiede l'autorizzazione per qualsiasi modifica ai dati. ☐
 - b. Assicura che i dati sono protetti da accessi non autorizzati. ☐
 - c. Assicura che i dati siano accessibili in qualsiasi momento. ☐
 - d. Valida l'identità di tutte le parti coinvolte. ☐
- 1.5 Quale dei seguenti potrebbe essere utilizzato come mezzo per nascondere del malware? **[1 punto]**
- a. File senza macro ☐
 - b. File smagnetizzati ☐
 - c. Rootkit ☐
 - d. Firewall ☐

- 1.6 Quale delle seguenti è una limitazione del software anti-virus? **[1 punto]**
- a. Viene disattivato quando l'utente è collegato a una LAN. ☐
 - b. E' necessario un firewall per attivare il software. ☐
 - c. Sono necessari aggiornamenti regolari per assicurare la massima protezione. ☐
 - d. Non può essere utilizzato per esaminare unità esterne. ☐
- 1.7 Quale dei seguenti viene utilizzato per impedire accessi non autorizzati di sorgenti esterne ad una rete? **[1 punto]**
- a. Rootkit ☐
 - b. Botnet ☐
 - c. Malware ☐
 - d. Firewall ☐
- 1.8 Quale delle seguenti icone rappresenta una rete cablata a cui è possibile collegarsi? **[1 punto]**
- a.  ☐
 - b.  ☐
 - c.  ☐
 - d.  ☐
- 1.9 Quale dei seguenti elementi indica che una pagina web è sicura? **[1 punto]**
- a. .org ☐
 - b. .edu ☐
 - c. https ☐
 - d. www ☐
- 1.10 Quale dei seguenti rappresenta delle informazioni di tipo testuale salvate dal browser quando si visita un sito web? **[1 punto]**
- a. Un cookie ☐
 - b. Un file di definizione ☐
 - c. Una backdoor ☐
 - d. Una macro ☐
- 1.11 Quale delle seguenti impostazioni NON può essere modificata quando si utilizza un sito di reti sociali? **[1 punto]**
- a. Informazioni sulle proprie abitudini e hobby. ☐
 - b. Celare il fatto di aver creato un account. ☐
 - c. Controlli sulla privacy che sono stati applicati. ☐
 - d. Le proprie informazioni e i contatti personali. ☐

- 1.12 Quale dei seguenti meglio descrive lo scopo della cifratura dei messaggi di posta elettronica? **[1 punto]**
- a. Viene utilizzata per verificare che il messaggio non contenga malware. ☐
 - b. Viene utilizzata per assicurare che il messaggio possa essere letto solo dal diretto interessato. ☐
 - c. Viene utilizzata nel phishing per distribuire messaggi a un gran numero di destinatari. ☐
 - d. Viene utilizzata per assicurare che i messaggi contenenti delle macro non contengano dei virus. ☐
- 1.13 Quale dei seguenti dovrebbe essere considerato una minaccia alla sicurezza durante l'apertura di un allegato a un messaggio di posta elettronica? **[1 punto]**
- a. Il file potrebbe contenere una firma elettronica. ☐
 - b. Il file potrebbe cancellare i cookie quando viene aperto. ☐
 - c. Il file allegato potrebbe richiedere una one-time password per poter essere aperto. ☐
 - d. Il file allegato potrebbe contenere una macro. ☐
- 1.14 Quale dei seguenti elementi può essere considerato una vulnerabilità della messaggistica istantanea? **[1 punto]**
- a. Identità biometriche. ☐
 - b. Hacking etico. ☐
 - c. Accesso tramite backdoor. ☐
 - d. Accesso in tempo reale. ☐
- 1.15 Quale dei seguenti NON è un metodo di distruzione permanente dei dati? **[1 punto]**
- a. Smagnetizzazione dell'unità che contiene i file. ☐
 - b. Cancellazione dei file dal disco. ☐
 - c. Triturazione del disco fisso. ☐
 - d. Riformattazione dell'unità contenente i dati. ☐

Salva e chiudi il file IT Security Sample Test Teoria.

Torna alla domanda 2 del test.