

Cognome: _____ **Nome:** _____ **Matricola:** _____

Sicurezza dei sistemi informatici e delle reti – 20 giugno 2013

Usa questa pagina per la brutta, staccala, non consegnarla.

Cognome: _____ **Nome:** _____ **Matricola:** _____

Sicurezza dei sistemi informatici e delle reti – 20 giugno 2013

Usa questa pagina per la brutta, staccala, non consegnarla.

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 giugno 2013

Tempo a disposizione: 60 (5 cfu) o 70 (6 cfu) minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

- 1. Attacchi ai sistemi di autenticazione.** Confronta gli attacchi on-line (in cui il prompt di login è accessibile via rete) e off-line (in cui il database utenti/password è disponibile in locale), compilando la seguente tabella con le tue considerazioni.

	On-line	Off-line
Quali sono gli strumenti tipici necessari ad un hacker per portare l'attacco?		
Fai delle considerazioni sul tempo necessario all'attacco.		
Elenca delle contromisure adottabili.		

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 giugno 2013

2. Sicurezza in azienda. Durante il tuo normale lavoro in azienda ti accorgi che un certo software X va in crash nel momento in cui si apre un file “fuori formato”. Il software X viene usato da gran parte dei dipendenti tutti i giorni ed è un prodotto commerciale non customizzato (per esempio è un famoso lettore di PDF).

2.1. Fai delle considerazioni tecniche circa la pericolosità di tale situazione.

2.2. Supponi che il tuo ruolo nell’azienda non sia in alcuna relazione con la sicurezza e supponi che esista un responsabile della sicurezza. Che cosa ti aspetti che faccia tale responsabile nel momento in cui viene a conoscenza del problema?

2.3. Supponi che non esista un responsabile della sicurezza. Che opzioni hai per dare un vantaggio

1. all’azienda
2. alla comunità
3. a te stesso (puoi elencare azioni “non-etiche” interessanti se ne conosci)

1. all’azienda
2. alla comunità
3. a te stesso

3. Web security. Descrivi brevemente i seguenti problemi di mostrandone un semplice esempio.

3.1. SQL injection

Descrizione:

Esempio:

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 giugno 2013

3.2. Non-persistent XSS

Descrizione:
Esempio:

3.3. Persistent XSS

Descrizione:
Esempio:

3.4. Cross site request forgery.

Descrizione:
Esempio:

4. IDS

4.1. Che significano “falso positivo” e “falso negativo”?

--

4.2. Secondo te sono più pericolosi i falsi negativi o i falsi positivi? Perché?

--

4.3. Considera un IDS di rete, discuti i problemi tecnici e le soluzioni relative all’installazione in una rete switchata.

--

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 giugno 2013

5. Rainbow tables

5.1. Qual'è la principale applicazione delle rainbow tables per un hacker?

5.2. Descrivi la struttura di una rainbow table e l'algoritmo di ricerca al suo interno.

Struttura:

Algoritmo di ricerca:

5.3. Qual'è la contromisura tipica per gli attacchi basati su rainbow tables?

6. [solo per 270] Windows security

6.1. Descrivi ciò che va in input al security reference monitor.

6.2. Esprimi brevemente il vantaggio e lo svantaggio di tale approccio rispetto a ciò che viene fatto in unix.

Vantaggio:

Svantaggio: