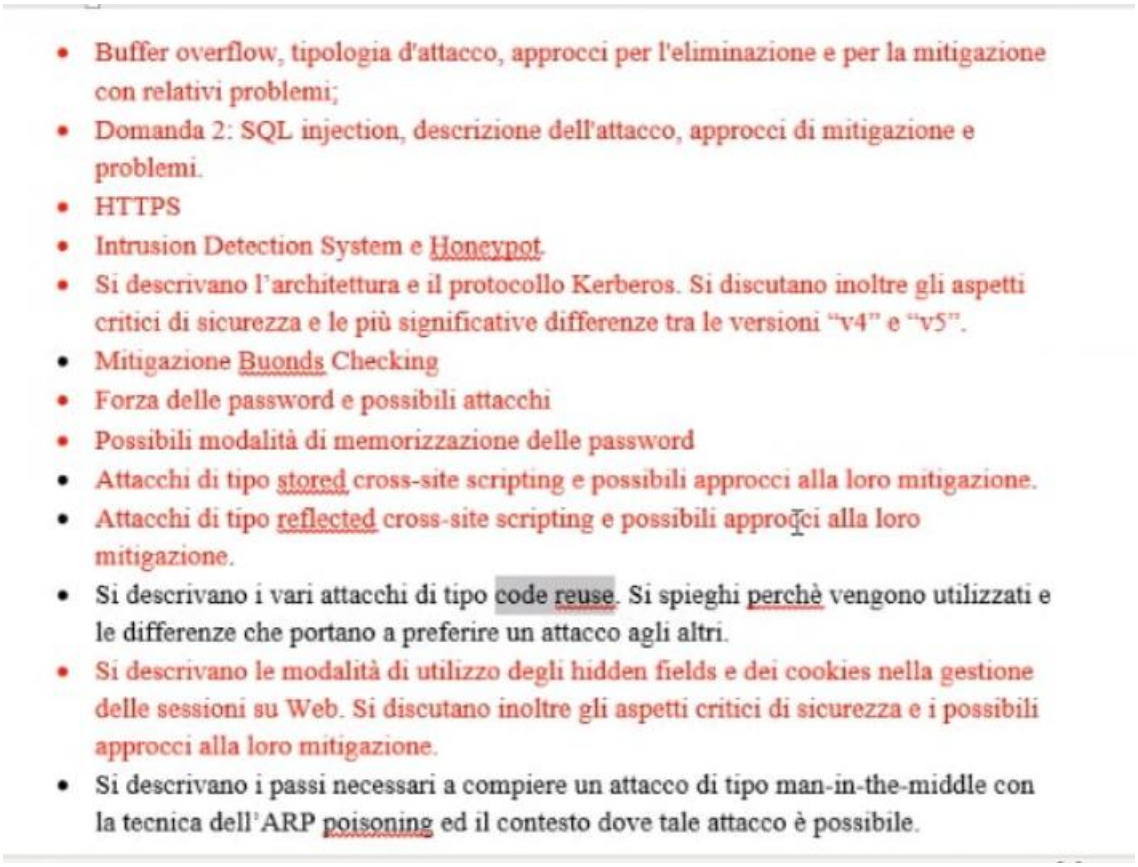
1)domanda teoria: bounds checking

2)domanda teoria: arp poisoning

La prima domanda era memorizzazione delle password

La seconda metodi per sovrascrivere la return address con lo stack canary



- Buffer overflow, tipologia d'attacco, approcci per l'eliminazione e per la mitigazione con relativi problemi;
- Domanda 2: SQL injection, descrizione dell'attacco, approcci di mitigazione e problemi.
- HTTPS
- Intrusion Detection System e Honeypot.
- Si descrivano l'architettura e il protocollo Kerberos. Si discutano inoltre gli aspetti critici di sicurezza e le più significative differenze tra le versioni "v4" e "v5".
- Mitigazione Buonds Checking
- Forza delle password e possibili attacchi
- Possibili modalità di memorizzazione delle password
- Attacchi di tipo stored cross-site scripting e possibili approcci alla loro mitigazione.
- Attacchi di tipo reflected cross-site scripting e possibili approcci alla loro mitigazione.
- Si descrivano i vari attacchi di tipo code reuse. Si spieghi perchè vengono utilizzati e le differenze che portano a preferire un attacco agli altri.
- Si descrivano le modalità di utilizzo degli hidden fields e dei cookies nella gestione delle sessioni su Web. Si discutano inoltre gli aspetti critici di sicurezza e i possibili approcci alla loro mitigazione.
- Si descrivano i passi necessari a compiere un attacco di tipo man-in-the-middle con la tecnica dell'ARP poisoning ed il contesto dove tale attacco è possibile.