- Dictionary attack
- Intern attack
- Osäkra meddelanden

Du skall skriva om ett hot i taget. Beskriv och förklara hotet, vad som händer under en attack och vad det innebär. Du skall sedan resonera och diskutera kring lösningar för hotet. Det finns inget krav för hur bra lösningen/lösningarna är, så länge du beskriver vad lösningen är, vad den hade löst och hur.

Dictionary attack

Genom Dictionary attack använder sig angriparen av en så kallad brute-force-teknik som innebär att man utgår ifrån vanliga ord och fraser som skulle kunna komma från en ordbok för att gissa lösenorden. Många människor använder sig av simpla lösenord just för att dom ska vara lätta att komma ihåg och på flera konton. Därför är Dictionary attack ofta framgångsrika då dom kommer åt flera konton och det krävs färre resurser för att lyckas. Det kan utföras både online och offline. Under en online attack försöker angriparen logga in upprepade gånger. Denna typ av attack kan upptäckas av systemadministratören eller användaren om den tar för lång tid. En offline attack har inga nätverksbegränsningar på hur många gånger som lösenordet kan gissas. Men för att kunna lyckas med det så måste angriparen kunna få access till lösenordsfilen från systemet vilket gör det mer komplicerat än en online attack. Lyckas det så kan angriparen logga in utan att det blir upptäckt.

Genom att uppmana användare att använda sig av unika lösenord med stor, liten siffra, tecken och fraser i sitt lösenord så kan man minimera risken för att det ska kunna hackas. Man kan kräva flerstegsautentisering och vid flertalet misslyckade försök kan man använda sig av kontoåterställning. Man kan använda sig av lösenordsbegränsning där det finns en lista ord som inte kan användas.

Intern attack

Innebär att någon som jobbar internt läckt lösenorden. Det kan vara svårt att förhindra men för att kunna spåra den som läckt kan man använda sig av logga för att se vilka eller vem som är inne på den specifika lösenordsfilen under tillfället den läcker.

Osäkra meddelanden

Okrypterade meddelanden och oautensierad kommunikation som leder till avläsning. Man kan uppmanas att klicka på en länk i ett mail där avsändaren ser ordentlig ut och länken inte avviker direkt vid första anblick med vid närmre koll så kanske det innehåller ett s för mycket. Vid klick på länken så kan de se identisk ut med original länken. Det är lätt att tro att man är på rätt webbsida men är helt enkelt i händerna på bedragarna. Det skapas en falsk trygghet.

Man kan förhindra detta genom att inte gå in på okända länkar. Och vara observant på avsändaren av meddelandet. Man kan även lägga till i tillexempel mobilen ett antivirus som meddelar att webbsidan är osäker och därmed stoppas du från att komma in på sidan och måste aktivt göra valet att lita på adressen eller källan.