PENETRATIONSTESTNING AV WEBBAPPLIKATIONER

Kandidatavhandling i datateknik

Alexander Tokos

Utkast 11.4.2018

Handledare: Dragos Truscan

Abstrakt

Webbapplikationer har på senare tid börjat ersätta program som förut fanns installerade på datorer. De är integrerade i våra liv i form av sociala medier och webbutiker. Även tjänster som förut krävde fysisk närvaro vid till exempel ett kontor så som banktjänster och statliga tjänster kan nu nås via webben.

Webbapplikationer hanterar en mängd känslig data så som lösenord och det är därför viktigt att denna data inte hamnar i fel händer. För att förhindra detta krävs det att webbapplikationen i fråga är säker.

Ett sätt att förbättra säkerheten hos ett program är utföra penetrationstest. Denna avhandling redogör för grunderna i penetrationstest. Målet är att analysera hur ett penetrationstest går till i praktiken. Som hjälp används Kali Linux, en Linuxdistribution som innehåller de viktigaste verktygen för penetrationstestning.

Sökord: penetrationstest, webbapplikation, Kali Linux

Innehåll:

1 Introduktion

[todo]

1 Webbapplikationer

En webbapplikation är i grund och botten ett datorprogram. Skillnaden mellan ett vanligt program och en webbapplikation är att en webbapplikation körs på en webbserver och kan användas via en webbläsare istället för att den körs och används på den dator man sitter framför [2].

1.1 Sårbarheter

[räkna upp relevanta sårbarheter]

1.2 Metoder för att upptäcka sårbarheter

Hur kan man försäkra sig om att en webbapplikation eller webbtjänst är säker? Det finns ett antal olika tillvägagångssätt. Denna avhandling kommer att handla om vad som ingår i ett penetrationstest och hur det går till specifikt för säkerhetstestning av webbapplikationer.

2 Penetrationstestning

Målet med penetrationstestning är öka säkerheten för ett datorsystem genom att försöka hitta sårbarheter i datorsystems säkerhet och utnyttja dessa sårbarheter för att angripa datorsystemet på samma sätt som en riktig hackare skulle göra. Penetrationstest utförs i de flesta fall med hjälp av samma verktyg och metoder som en potentiell, illasinnad angripare skulle dra nytta av. Genom att ta i beaktande penetrationstestets resultat kan man åtgärda säkerhetsbristerna innan systemet blir angripet på riktigt [1].

2.1 Penetrationstestningsprocessen

Det är viktigt att ett penetrationstest är genomförligt så att så många säkerhetsbrister som möjligt hittas och kan åtgärdas. Detta kräver att testet utförs på ett strukturerat och genomtänkt sätt [1].

Patrick Engebretson förklarar i sin bok *The Basics of Hacking and Penetration Testing* [1] fyra steg som utgör grunden för penetrationstestningsprocessen. I nästa del av detta kapitel förklaras stegen som hör till ett penetrationstest.

2.1.1 Rekognoscering

2.1.2 Identifiera sårbarheter

2.1.3 Utnyttja sårbarheter

2.1.4 Upprätthåll tillgång

2.1.5 Rapport

Det viktigaste i ett penetrationstest enligt Engebretson är den slutliga rapporten. I den ingår allt som gjorts under testet, alla relevanta upptäckter angående säkerheten samt eventuella rekommendationer på förbättringar i systemet [1].

2.2 Typer av penetrationstest

[black-, white- och grey box test]

Diskussion