Opponering på DATX02-12-29
av DATX02-12-06

Sammanfattning av projektet
Arbetet "Dubbla nätverk i samma dator" består av en undersökning som går ut på att ta reda på om det går att få god säkerhet med hjälp av två virtuella nätverk kopplade till två virtuella maskiner i en dator. I systemet de virtuella maskinerna ingår i finns ett intranät och ett externt nätverk med internetåtkomst. Den ena maskinen ska endast kunna komma åt intranätet och den andra ska endast komma åt det externa nätverket.

Gruppen har genomfört en omfattande litteraturstudie för att undersöka de säkerhetsbrister som kan uppkomma vid virtuella nätverk. Gruppen har efter litteraturstudien genomfört tester för att testa säkerheten hos systemet. Ett antal olika konfigurationer av mjukvara har genomförts för att jämföra prestanda och säkerhet.

Arbetet har resulterat i en konfiguration som upprätthåller en god säkerhetsnivå mellan de två olika nätverken. Tyvärr ger den delade hårdvaran möjlighet till prestandaförändringar som kan påverka det andra nätverket. Gruppen anser att lösningen inte ger samma säkerhet och prestanda som två fysiskt separerade nätverk.

Allmänt om rapporten
Rapporten är välskriven och följer en lättläst struktur. Den beskriver kort och koncist arbetets gång och resultat. En undersökning som den beskriven i rapporten kräver en omfattande litteraturstudie. Arbetet innehåller många bra och relevanta referenser och ger en känsla av en grundlig litteraturstudie. Tyvärr saknar rapporten en del teori vilket ger ett ytligt intryck. Exempelvis skulle teoriavsnittet kunna utökas med information om hubbar, switchar och routrar.

Det känns som omfattningen av arbetet var begränsad. Den utförda testningen av systemen beskrivs så kortfattat att det inte ger en känsla av dess omfattning. Mer teori och utförligare genomförande kunde hjälpt till med att framhäva vad gruppen kom fram till. I rapporten framgår det tydligt att gruppen har lyckats med att uppfylla arbetes syfte och dess mål.

Upplägg och struktur

Rapporten känns välstrukturerad med tydliga huvudrubriker. Innehållet kommer i en ordning där nödvändig teori ges innan den används i texten.

Sammanfattning och *Abstract* är två kapitel som visuellt ger en estetiskt tilltalande känsla vid första anblicken. De smala rektanglarna formade av text ger en professionell känsla. Tyvärr gör den smala bredden på texten att nästan varje ord klipps vid slutet av raden. Det gör att materialet blir svårläst. Då texterna saknar styckesindelningar är det lätt att tappa bort sig. Även under kapitlet *teori* skulle fler styckesavdelningar göra läsningen lättare. Nu är det endast rubrikerna som avdelar texten.

Nedan följer fler iakttagelser angående rapportens upplägg och struktur:

- Det känns tveksamt om kapitel 1.7 *Rapportstruktur* behövs överhuvudtaget. Kapitlet beskriver egentligen bara samma sak som innehållsförteckningen.
- I kapitlet 2.2 *Nätverkslagren* står texten "Inom ramen för detta projekt...". Detta är inte teori och stycket borde stå under konfiguration.
- Kapitel 5.1 *Beskrivning av attacker* innehåller information om de tre olika sorters attacker som användes under undersökningen. Informationen om dessa innehåller bara fakta och inget som faktiskt som tillhör genomförande. De tre olika texterna borde flyttas till teoriavsnittet.

- Kapitel 5.3 heter *Resultat av attacker* och borde som namnet antyder ligga under resultatkapitlet.

Innehåll

Innehållet gav för det mesta en god bild av det som förklarades. I en del fall kändes teorin bakom vissa saker är bristfällig. Som exempel nämns det aldrig vad ett subnät är eller hur det påverkar IP-adressers spann. En annan sak som inte nämns är varför det använda adresspannet (192.168.1.0) av ip-adresser valdes. Det finns fler adresspann som kan användas för undersökningar av denna typ, till exempel 172.16.0.0. Likaså anses teori om hubb, switch och router borde förklaras för att kunna förstå hela rapporten fullt ut.

Det var bra skrivet i *1.8 Terminologi* att svenska ord används där det finns en vedertagen svensk översättning. Dock kändes det som att detta inte alltid efterföljdes, till exempel när det skrivs om olika virtualiseringslösningar.

Teorikapitlet om virtualisering är välskrivet, det framgår bra hur olika metoder och tekniker fungerar. Det enda som skulle kunna vara tydligare är att förklara vad det innebär att mjukvara kan köras direkt på hårdvaran.

Kapitel 5.3 *Resultat av attacker* innehåller många termer och är en tekniskt svår del i rapporten. Det är lätt att tappa bort sig med alla olika konfigurationer som nämns. Det skulle kanske vara bättre att tydligare dela upp resultatet för de olika konfigurationerna och på så sätt göra det lättare för läsaren att förstå. De tabeller som finns hjälper till på ett bra sätt med att lösa problemet.

Nedan följer fler iakttagelser angående rapportens innehåll:

- På framsidan av rapporten är gruppens nummer ej inkluderat. Det står "nr 2012:000".

- Under kapitel 2.3.2 *Protokollet 802.1Q* står ingen argumentation om varför VLAN kan köras utan taggar. Då en stor del av resultatet beror på att VLAN kan köras utan taggar hade mer teori om detta varit av godo.

- I kapitel 4.4 *Överbelastning av systemen* beskrivs det vad är överbelstningsattack är för något och hur den fungerar men det står inget om att det är en DoS (Denial of Service) attack.

- Tabellen på sida 32 stämmer inte överens med resultatet i texten.

- I stycket i kapitlet 7.1 *Evaluering av miljön* diskuteras resultatet bra, det är en bra diskussion runt andra alternativ och kompletteringar som skulle var möjligt att göra för att stärka säkerheten. Det känns dock som att det saknas en förklaring kring varför kryptering och brandvägg skulle vara ett bra alternativ.

Språk

Överlag känns språket i rapporten formellt, dock varierar stilen genom rapporten en del. Det märks ibland att rapporten är skriven av olika personer. Detta eftersom ord som till exempel "man" bara förekommer i vissa stycken och källhänvisningar ser annorlunda ut vid olika delar av rapporten.

Referenser

Referenserna i rapporten är mycket goda. Eftersom rapporten använder sig av Vancouversystemet känns det konstigt att referenser som "[5] skriver att..." dyker upp. När referenser är så opersonliga som de är enligt Vancouversystemet känns det mer naturligt att läsa referenser placerade i slutet av meningar eller stycken.

Nedan följer fler iakttagelser angående rapportens referenser:

- Under vissa stycken refereras det till samma källa flera gånger. Detta gör texten hackig. Det är bättre att skriva referensen en gång i slutet av stycket.

- Det är tydligt att gruppen har gjort grundliga litteraturstudier då källorna både är många och relevanta för arbetet

Avslutning

Rapporten berör ett tekniskt avancerat område på ett intressant och lättläst vis. Texten har ett bra flyt som får läsaren att bli intresserad av ämnet. Det finns några få saker att anmärka på i texten, men över det stora hela är det en bra rapport.