Christer Hamberg ch222xb

Opponeringsrapport Över Rikard Österlunds Kandidatarbete

Arbetet är ett mycket välskrivet arbete. Språket är bra, välstrukturerat och sakligt relevanta tekniska termer för en Linux användare förekommer (free, malloc, realloc osv.) vilket gör det enkelt att följa texten. Även uppbyggnaden av texten är saklig och det blir som att läsa en dagbok.

På grund av detta får man snarare söka efter fel än att man enkelt kan finna dessa i texten. Det finns några mindre stavfel t.ex. kapitel 1.1.1 i sista stycket ”…från processer som *försöka* skriva…. ” ska det vara *försöker* istället. I Kapitel 1.3 står det ”*En typisk fall*…” som ska vara ”*Ett typiskt fall*…”

Men eftersom texten är så välskriven så spelar dessa ingen roll, och jag finner inte att det skulle tillföra så mycket att haka upp sig på dylika petitesser.

Frågan är mycket aktuell med tanke på att med olika containerslösningar och molnlösningar ökar antalet fall där man skulle kunna tänka sig att en utomstående kan få access till minnet, utan att ha fysisk access till det. På detta sätt kan dessa alltså få tillgång till data som de inte borde ha tillgång till

Förbättrings förslag

Eftersom rapporten är mycket saklig finner jag det bättre att fokusera på förslag som skulle kunna göra rapporten ännu bättre. Vissa saker kan säkert inte göras eftersom de skulle ta lång tid att utreda, men i så fall kanske man skulle kunna tänka sig att de kanske kan vara framtida forskningsobjekt.

1. Rapporten tar upp ett sakligt ämne, dock kräver ju detta fysisk access till själva minnet i maskinen. Så skulle det ev. vara bättre att fokusera studien även på de processer som kan få åtkomst till minnet utan att man har fysisk access till DIMMarna. Detta kan vara ett framtida forskningsprojekt.

   För att på ett bättre sätt beskriva den fråga som jag ställde, men en ganska klumpig formulering så: I en molnlösning kan man köra containers från flera olika kunder på en och samma fysiska server, minnet är ju gemensamt för hela servern. Studien visar ju på att minnet inte raderas, dvs. Om jag är ute och snokar efter andras lösen ord kan ett sätt att komma åt dessa vara att starta en applikation i sin egen container som ligger och allokerar minnesblock och efter att minnesblocket blivit allokerat så läser man bara igenom det för att se vilka ”rester” som det innehåller. Hittar man inget, deallokerar man minnet, och allokerar ett nytt block (lite större storlek så att man troligen får en annan minnesarea) och så gör man om sökningen. På detta sätt skulle man skapa en ”minnessniffer” som ligger på servrarna och bara skummar av minnet i hopp om att hitta något intressant.

   Dock, inser jag efter presentationen att detta ligger utanför den genomförda studien men kan ev. vara ett fortsatt forskningsobjekt.

2. Rapporten är skriven på Svenska, genom att skriva rapporten på Engelska skulle rapporten vara synlig och tillgänglig för en bredare forskarpublik, detta borde egentligen vara ett krav från LNU.
3. Det finns ett par begrep som kan vara bra att reda ut för en person som inte är insatt i frågorna, dvs. *volatile, virtualbox*
4. Rapporten beskriver en studie runt det som man tala om som cold boot attac, det skulle ha varit bra att ta upp detta som ett begrepp,
5. Andra sätt att komma åt minnet, dvs. ptrace() komma åt processer / skydda minnet. Användandet av mlock () för att förhindra swap till disk osv. Kunde eventuellt ha varit med som alternativa lösningar.
6. I 1.6 Avgränsningar finns det i slutet ett omnämnande att till stor del utelämnats, vilka delar har inte utelämnats resp. utlämnas? En del av detta täcktes i den muntliga presentationen.
7. 2 Metod frågorna besvaras med Ja/Nej men det finns även ett Delvis med i resultatet, behövs detta förtydligas?
8. 2.1 metodbeskrivningen Fråga 3 här nämns en Litteraturstudie, vilken är den?
9. Under metodbeskrivning 2.1 Beskrivs fråga 1, 3 och 4. Fråga 2 har utelämnats i beskrivningen, vilken metod har använts för att besvara denna, behövs den beskrivas?
10. 3 Resultat VirtualBox beskrivs inte, kan användningen av den ha påverkat resultatet.
    SVAR: Nej, detta kom fram under den muntliga presentationen.
11. Program beskrivningen Kod3.1 borde eg. vara inläsning, inte avläsning.
12. I analysen eller exekveringen, eftersom man avsöker hela minnet hur säkerställde man att det inte redan innan exekveringens början inte fanns ”rester” av lösenorden i minnet?
    Besvarades under den muntliga presentationen, kan vara bra att förtydliga de unika lösen ord som alltid användes.
13. 6.1 Framtida forskning, borde man göra en djupare analys eller jämföra mellan olika kompilatorer hur detta fungerat? Mellan olika operativsystem? Mellan olika programmeringsspråk (Java, CSharp os)
14. 6.1 Framtida forskning borde man nämna att en djupare forskning hur man kan komma åt informationen utan att ha fysisk access till minnet (mlock, ptrace)?
15. Har TRESOR eller en TRESOR liknande lösning ev. kunnat lösa problemet? (Lagrar i CPUns register istället för i RAM) Är en patch till Linux kerneln. Dock kommer den med sina egna utmaningar både overhead samt begränsning i tillgängliga register.
16. Som forskare hur skulle du lösa problemet?
    Bra svar under presentationen!!

En mycket bra presentation och det är några saker som kan förtydligas om du känner att de tillför något. Personligen skulle jag bearbeta framtida forsknings kapitlet lite eftersom det finns en rad områden som man kan studera och jämföra resultatet av med den skrivna rapporten.

Ett mycket bra arbete!