Laboration 4

Attacker mot system behöver inte vara av generell art (som tex. sub7) utan kan i värsta fall vara designade mot just det företag som du företräder. Under denna labb ska vi försöka analysera en specialdesignad trojan som inte upptäcks av virusskydd eller andra automatiserade verktyg. Börja med att kopiera upp foldern Lab 4 från D:\VMW_template. Starta upp den virtuella maskinen och vänta på att det ska starta. Vi antar att vi redan genomfört initial respons och forensisk avbildning och att vi nu har möjligheten att provköra datorn som en virtuell maskin, utan risk för att vi förvanskar några originalbevis. Behöver du root-access så är lösenordet ”forensics”.

Kontroll av portar
Vi börjar med att göra en undersökning av systemets aktiva portar. Detta görs med ”sudo netstat –anp”. Detta leder till att vi får en lång lista med information om vilka portar som är aktiva på systemet och vilka processer som är kopplade till dessa. Vi skulle nu kunna gå igenom alla rader i listan, en och en, och undersöka vilka som verkar vara misstänkta, men detta är för omständligt och vi måste begränsa urvalet något. Om det är så att den eventuella trojanen tillåter att man fjärrstyr den infekterade datorn så kan man förvänta sig att det öppnats en port för inkommande trafik. För att begränsa oss kan vi sortera ut rader med hjälp av en pipe till ”grep LISTEN”. Ett begränsat antal rader kommer att visas. Fundera ut vad det är som inte stämmer. (ledtråd: börja uppifrån) Anteckna portnumret som processen använder.

Processinfo
När du kör netstat så får du förutom processens namn även process-id (PID). Med hjälp av PID kan vi sedan ta reda på hur processen startades. Denna information hittar du i foldern /proc/PID/, där filen cmdline innehåller den kommandorad som startade processen (använd ”cat” eller ”nano”). Anteckna sökvägen till processen.

Provokation
Innan vi går vidare med att bryta ner trojanen så ska vi provocera den lite och se om den svarar. Vi vet på vilken port den lyssnar och kan prova att koppla upp oss med telnet på den porten (”telnet localhost PORT”). I det här fallet svarar trojanen och vi dokumenterar detta.

Analys
Nu kan vi gå vidare med analysen av koden. Man kan i det här läget analysera själva programkoden med hjälp av en debugger, ett verktyg som möjliggör stegvis analys av koden medans den körs. Detta kräver dock expertkunskaper i programmering och är kanske i många fall onödigt komplicerat. Har man tur så kan en enkel sökning i själva datafilen faktiskt göra att man hittar vad man letar efter. Vi börjar med att analysera trojanfilen som vi nu lokaliserat. Detta görs med kommandot ”file FILNAMN”. Resultatet du får berättar hur filen är kompilerad, men det som är viktigast är att det faktiskt är en exekverbar fil och att den inte innehåller någon teckeninformation (stripped). För att undersöka innehållet i filen kan man antingen använda sig av ett visarprogram som tex. hexview (”hexview –C FILNAMN”) eller strängutvinning (”strings FILNAMN”). Gör vi det så får vi reda på att filen är packad med UPX, ett program som används för att packa körbara filer så att de packas upp med automatik när de ska köras. Baksidan med detta är att dels så ändras filens checksummor och går på så vis att gömma för antivirusprogram och dessutom så kodas det ursprungliga innehållet i filen på ett sätt som gör att det inte går att läsa innehållet i klartext. Som tur är

går det även att packa upp filer med hjälp av UPX (upx –d FILNAMN) och på så vis återställa den ursprungliga filen.

Gör vi nu en analys av filen med hjälp av ”file FILNAMN” så kan vi se att filen inte längre är ”stripped”. Gör vi strängutvinning på nytt så kan man se att det nu finns en hel del information lagrad i filerna. Det är dock för mycket data för att göra en fullständig manuell sökning – vi måste få hjälp med att veta vart vi ska börja leta. För att underlätta sökningen i filen föreslår jag att ni gör en strängutvinning och dirigerar utdatat till en ny fil ni kan öppna i gedit. Som sökuttryck kan ni använda den respons som vi provocerade fram tidigare. Undersök strängarna i närheten av träffarna du fick – du bör hitta en del text som du inte sett under provokationen. Anledningen till detta är att om programmet innehåller ett hårdkodat lösenord så kommer det troligast att finnas bland alla andra strängkonstanter i programmet. För skojs skull så kan vi koppla upp oss med telnet på nytt och prova några som lösenord och hoppas på det bästa. Kan vi inte hitta det efterfrågade lösenordet i klartext så återstår tyvärr endast att analysera koden i en debugger och antingen lista ut hur lösenordet beräknas eller förändra koden så att lösenordet inte efterfrågas (detta ligger utanför kursens omfattning).

Nu vet vi vad den körbara filen heter, vi vet på vilken port den arbetar, vi vet hur man använder den och även vilket lösenord som fungerar. För att komplettera detta så ska vi undersöka om trojanen använder sig av några externa filer (tex. konfigurationer). För att göra detta så börjar vi med att avsluta den körande trojanen och starta om den med hjälp av strace (”strace FILNAMN”). **OBS! Använd absolut sökväg.** (varför?) Med hjälp av strace kan vi se alla systemanrop som programmet gör. För att läsa in en konfigurationsfil måste man använda sig av någon form av inläsningsfunktion och troligtvis använder man sig av något som systemet redan tillhandahåller. Om ni letar igenom strace-loggen så kan man se att trojanen faktiskt öppnar en konfigurationsfil (open). Kontrollera filens innehåll. Har man tur så kan den innehålla mycket intressant.

Rensning
Nu har vi gjort en grundläggande nedbrytning av ett okänt program och vi kommer inte längre utan att detaljanalysera koden i en debugger. Men vi har samtidigt fått ett stort antal uppslag på filer att undersöka i ett verktyg som Autopsy. Antagligen så kör man en version av den avbildade datorn i VMWare medan man kör en avbild i Autopsy och använder uppslagen man får i emulatorn för att styra hur analysen i Autopsy ska gå tillväga.

Kontrollera om trojanen kör på systemet (”sudo ps aux”). Om den kör ska den nu dödas. Avvakta ett par minuter och kontrollera att processen inte körs. Varför beter den sig så? Fundera ut hur du ska rensa ut trojanen från systemet. Ett litet tips finns i trojanens konfigurationsfil. Vilka andra filer ska tas bort? Kontrollera vad som händer om du tar bort trojanen. Prova att koppla upp dig med telnet på nytt. Vad är det som händer? Om vi lyckas rensa systemet från trojanen, kommer det vara komplett och körbart efter detta? Är det lämpligt att åtgärda felen hos systemet och starta upp det igen?

Stäng ner och ta bort den virtuella maskinen på vanligt vis.

Demonstration (utgår)
LiveView