Projektnummer/Project no
E716589
Uppdragsgivare/Client
Försvarsmakten
FoT-område
Operationer i cyberdomänen

Författare/Author
Oliver Johansson

Datum/Date
2022-12-23
Memo nummer/Number
FOI Memo 8085

Användartester för teknisk informationshämtning i Lore GUI

1 Bakgrund

I projektet *Verktyg och teknik för CNO-övningar* används en uppbyggd kunskap inom intrångsdetektion och logganalys för att utveckla verktyg relaterat till *Computer Network Operations* (CNO) i syfte för övningar och tester. Ett av dessa verktyg är *Lore* som automatiserar cyberangrepp under cybersäkerhetsövningar. I projektet har ett användargränssnitt till Lore utvecklats för att kunna skapa, redigera och starta Lore-scenarier samt kunna se loggar och resultat från exekverade scenarion. Användargränssnittet kommer i detta memo att kallas för Lore *Graphical User Interface* (GUI). I memot beskrivs det användartest som genomförts för att undersöka hur intuitivt användargränssnittet är i relation till att hämta teknisk information vid förberedelser, initiering och tolkning av resultat från scenarier.

1.1 Lore

Lore är ett verktyg utvecklat av *Totalförsvarets forskningsinstitut* (FOI) för att automatisera cyberangrepp under cybersäkerhetsövningar. Med hjälp av Lore kan en operatör skapa anpassningsbara scenarion som specificerar angripare, kallade röda profiler, vars mål är att kompromettera angivna mål. Scenarion går att justera med en mängd olika parametrar, exempelvis tillåtna handlingar, vilka virtuella datorer/nätverkssegment som bör uteslutas, vilken förkunskap angriparen har och vilka algoritmer som bör användas för att ta beslut vid olika handlingar. [1]

Under exekvering behövs ingen användarinteraktion. Med det sagt är det möjligt för en operatör att ändra på parametrar för ett scenario under dess exekvering, såsom att lägga till ny kunskap manuellt, prioritera upp särskilda handlingar eller byta ut mål. [1]

Att justera och anpassa scenarion till olika lärandemål kräver ingen särskild specialkompetens, samt anses vara både enkelt och billigt [1]. Däremot är Lore ett avancerat verktyg som kan vara svårförståeligt för en oerfaren operatör. För att minska tröskeln för att förstå och nyttja verktyget har användargränssnittet Lore GUI utvecklats. Användartester har sedan gjorts för att se om gränssnittet fyller dessa behov.

1.2 Användartester för användargränssnitt

Användartester för användargränssnitt är en process inom utveckling av *User Experience* (UX) för att testa användarupplevelsen i praktiken och se om det testade gränssnittet uppfyller en användares behov. Till skillnad från enhets- och integrationstester som testar applikationens funktionalitet, kan inte användartester effektivt testas automatiskt. Vid UX-utveckling kan det ingå subjektiva val och rena gissningar vid implementation av användargränssnitt. Detta innebär att testerna behöver utföras av människor för att verifiera interaktivitet och tydlighet, beroende på användargränssnittets syfte.

Lore är ett expertsystem inom cybersäkerhet vars primära användningsområde är inom cybersäkerhetsövningar där målgruppen är personer med kompetens inom cybersäkerhetsområdet. Därför har användartestet som beskrivs i detta Memo fokuserat på att testa Lore GUI utifrån hur intuitivt det anses vara för att hämta teknisk information för målgruppen inom FOI.

2 Lore GUI

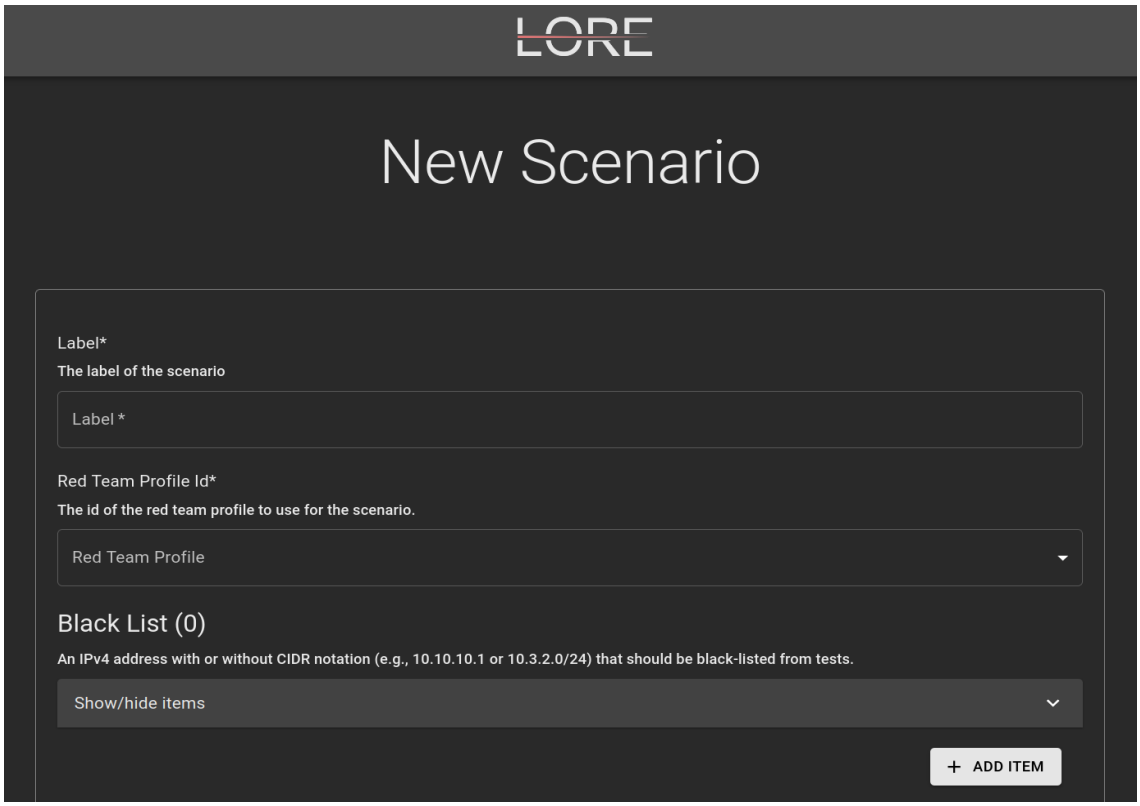
Lore GUI är en webbapplikation skriven i *React*, ett JavaScript-bibliotek för att utveckla grafiska gränssnitt. Syftet med användargränssnittet är att förbättra användarupplevelsen av Lore i syfte att göra verktyget mer intuitivt och informationshämtningen smidigare. Vid användartesternas utförande fanns följande funktionalitet i Lore GUI:

- Skapa och redigera scenarion
- Exekvera, stoppa och pausa scenarion
- Skapa och redigera röda profiler
- Visa kunskapsdatabas för instanser av scenarion
- Visa mål och målstatus för scenarion

Varje funktionalitet beskrivs i kommande avsnitt.

2.1 Skapa och redigera scenarion

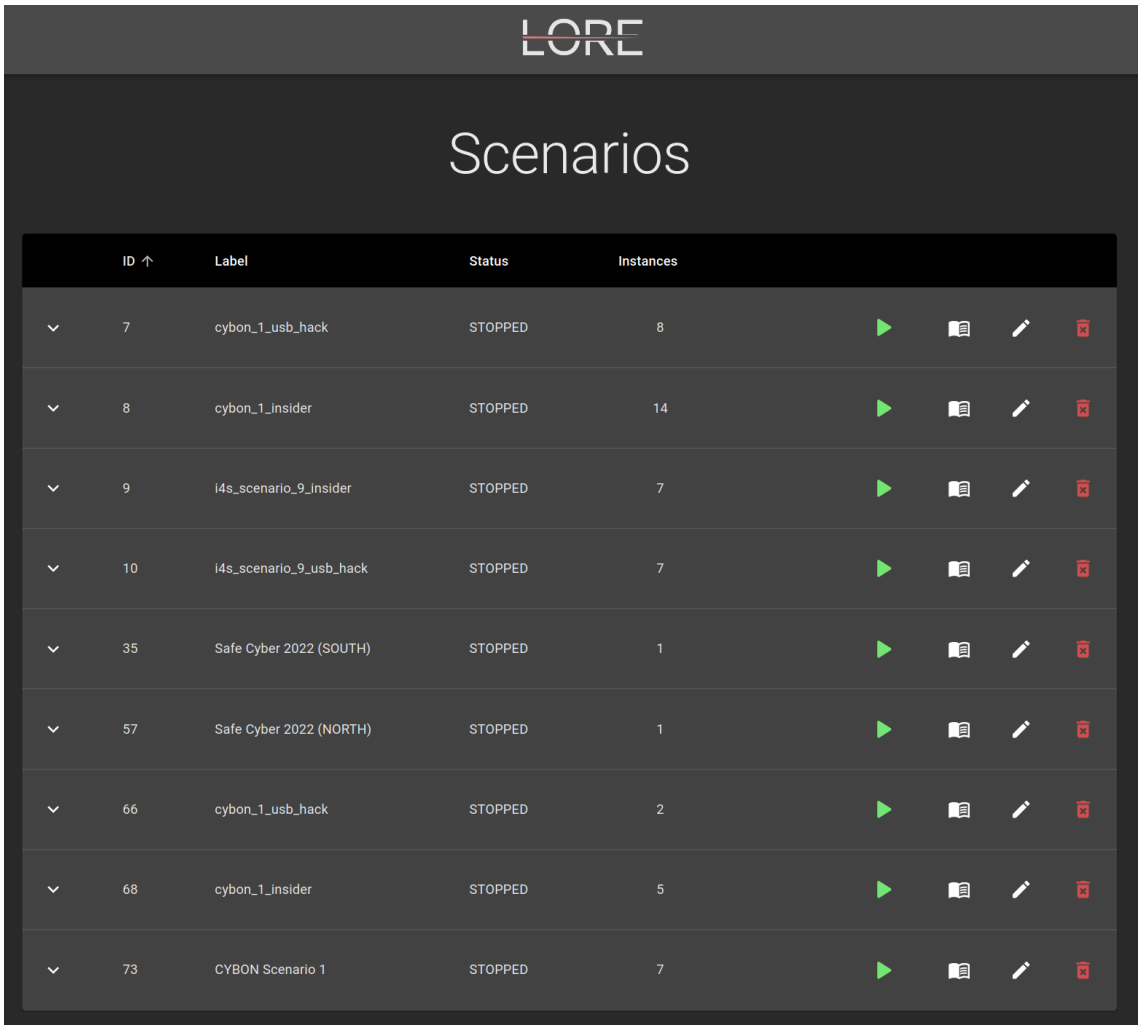
Scenarion är en väsentlig del av Lore, att skapa och redigera scenarion är därför två viktiga funktioner i Lore GUI. Scenarion går att skapa eller redigera via två typer av formulär i användargränssnittet, ett formulär som visar samtliga parametrar och ett förenklat formulär som endast visar de mest nödvändiga parametrarna. Anledningen till att det finns två olika formulär är att det inte är nödvändigt för en oerfaren operatör att se alla parametrar, men möjligheten att kunna justera dem i scenarion ska dock fortfarande finnas. I Figur 1 visas vyn för att skapa ett scenario via det förenklade formuläret i Lore GUI.



Figur 1: Formulär för ett nytt scenario i Lore GUI.

2.2 Exekvera, stoppa och pausa scenarion.

Alla scenarion i Lore kan visas som en lista i användargränssnittet, se Figur 2. I listan finns information om varje scenario, samt ett antal knappar där en operatör bland annat kan ta bort, redigera och exekvera ett scenario. Om ett scenario redan exekveras kan operatören även stoppa eller pausa det.



Figur 2: Lista över scenarion i Lore GUI

När ett scenario exekveras skapas en instans, som också visas i scenariolistan. En operatör kan se alla instanser i ett scenario genom att klicka på pilen längst ut till vänster för ett givet scenario, vilket expanderar en lista över alla dess instanser.

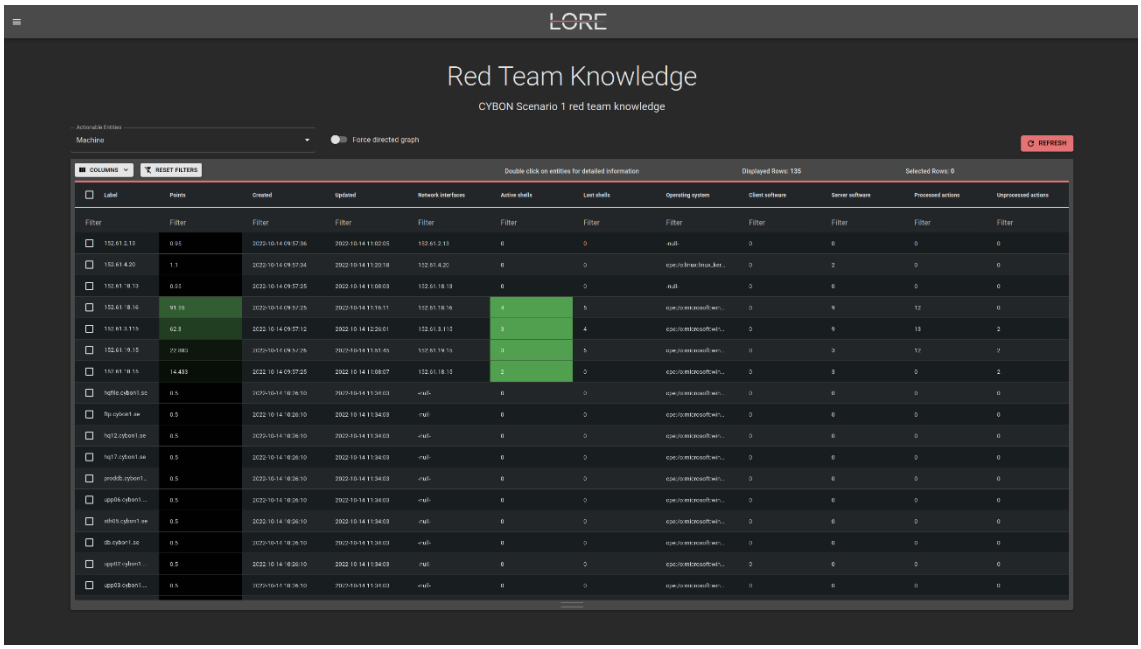
2.3 Skapa och redigera röda profiler

Röda profiler kan likt scenarion också skapas och justeras via formulär i Lore GUI, som i Figur 1. Till skillnad från scenarion finns endast ett formulär för röda profiler, som innehåller samtliga parametrar. Anledningen till att det inte finns något förenklat formulär för röda profiler vid användartesternas genomförande är för att oerfarna operatörer inte har lika stort behov av att kunna skapa eller redigera röda profiler jämfört med scenarion. Röda profiler kan enkelt återanvändas i olika scenarion och kan vid behov förberedas i god väg innan av mer erfarna operatörer.

Alla röda profiler kan också visas som en lista likt i Figur 2. På samma sätt som för scenariolistan går det att redigera och ta bort röda profiler. Däremot saknas det funktioner som är exklusiva för scenarion, som till exempel att exekvera scenarion och visa instanser.

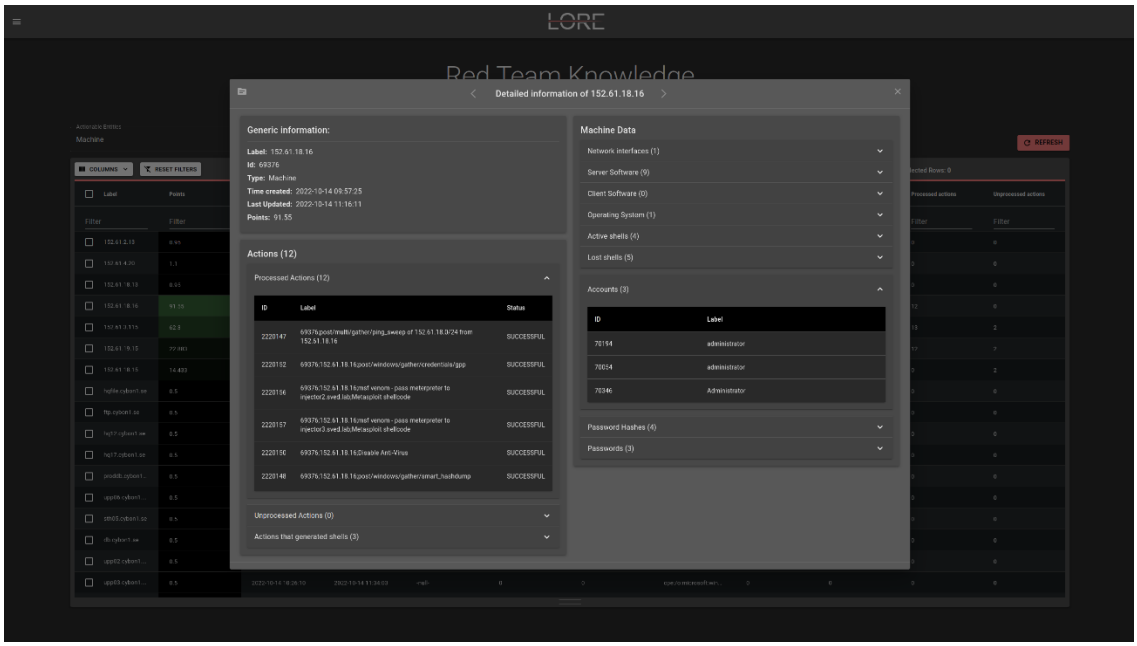
2.4 Visa kunskapsdatabas för scenarion och instanser

Varje scenario och scenarioinstans har en kunskapsdatabas över all information som har samlats in under en exekvering eller tilldelats innan exekvering. Den här informationen går att visualisera i Lore GUI genom en övergripande tabell, se Figur 3. Kunskapsdatabasen kan innehålla flera olika typer av entiteter, exempelvis virtuella datorer eller nätverkssegment. Endast en entitetstyp visas i tabellen åt gången, vilken bestäms av en rullista ovanför tabellen. För att hjälpa operatören att söka efter specifika entiteter går varje kolumn att sortera och filtrera med vanlig text eller reguljära uttryck (Regex).



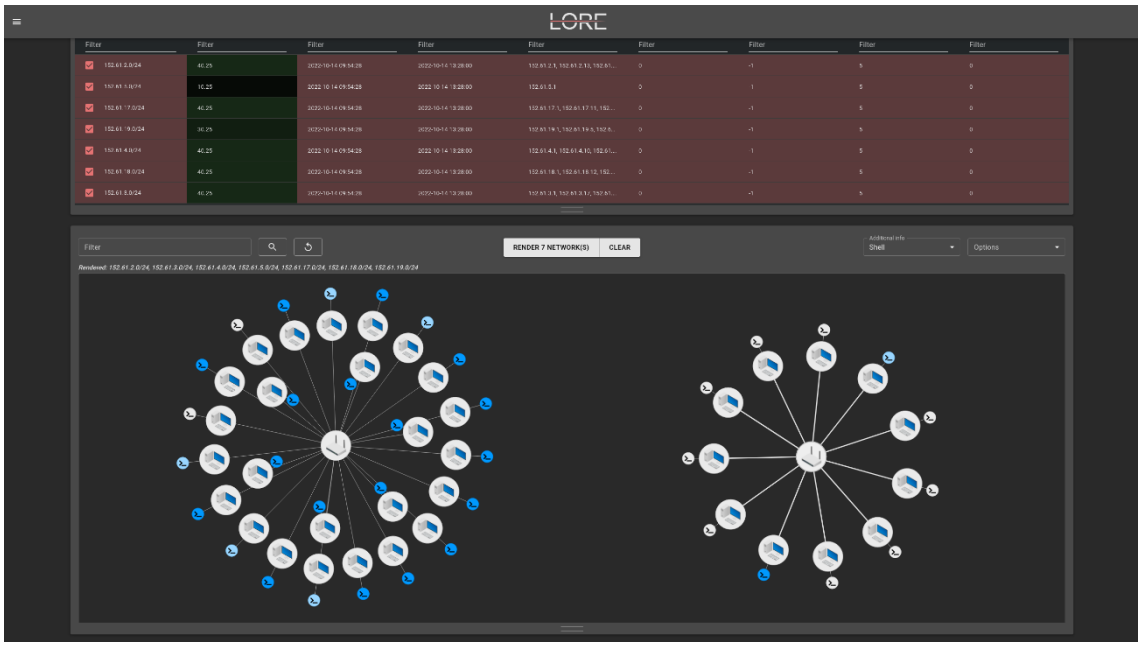
Figur 3: Kunskapsdatabasen över en scenarioinstans i Lore GUI

I tabellen visas inte fullständig information för varje entitet, eftersom det skulle göra tabellen svårläst. Däremot är varje entitet i tabellen klickbar för att visa en dialogruta som innehåller detaljerad information om enheten, samt relaterade entiteter. Figur 4 visar ett exempel på en sådan dialogruta.



Figur 4: Entitetsdialog i Lore GUI

Entiteterna i den övergripande tabellen går även att visualisera som nätverksdiagram för att se relationer mellan olika entiteter. I nätverksdiagrammet kan specifik information för entiteter visas för att få en överblick av en viss variabel, exempelvis om en maskin har blivit komprometterad eller inte (se Figur 5).



Figur 5: Nätverksdiagram för olika nätverkssegment och maskiner i Lore GUI

Den övergripande tabellen, dialogen med detaljerad information och nätverksdiagrammet är de tre olika sätt som kunskapsdatabasen i Lore GUI kan visualiseras på. En operatör kan använda dessa funktionaliteter enskilt eller i kombination med varandra för att undersöka och tolka utfallet av ett scenario.

3 Metod

I det här kapitlet beskrivs arbetet inför och under användartesterna som undersökte hur intuitivt Lore GUI är för att hämta teknisk information. Kapitlet kommer inte undersöka implementationen av användargränssnittet.

Inför användartesterna behövde tre frågor besvaras:

- Vad ska testas i användargränssnittet?
- Hur ska användartesterna utföras?
- Vilka personer ska delta i testerna?

Användargränssnitt går att granska ur flera perspektiv men det som undersöks i ett användartest bör alltid vara relevant för användargränssnittets ändamål. Då syftet med Lore GUI är att tydligare förmedla teknisk information till operatören och förenkla interaktiviteten med Lore ansågs teknisk informationshämtning som en relevant aspekt att undersöka under användartesterna.

Användartestet utformades i form av uppgifter som testdeltagarna skulle utföra i användargränssnittet, där uppgifterna skulle spegla vanliga arbetsuppgifter en operatör skulle kunna ha i Lore GUI. Därför hade uppgifterna som mål att nyttja de funktioner som ansågs vara viktigast och mest förekommande i användargränssnittet.

Ett antal uppgifter skapades baserade på de scenarioinstanser som fanns tillgängliga i databasen för Lore. Utifrån de skapade uppgifterna valdes några stycken, som vidareutvecklades tills de ansågs vara tillräckligt tydliga och relevanta för användartestet. Totalt skapades 20 stycken deluppgifter uppdelade i de fem kategorierna: skapa scenario, redigera scenario, starta/stoppa scenario, tolka kunskapsdatabas och tolka mål. Utöver uppgifterna utformades enkla instruktioner om användartestets utförande. Alla frågor och instruktioner var utformade för att kunna presenteras direkt till testdeltagarna i form av ett utskrivet papper under användartesterna. Detta för att säkerställa att alla testdeltagare skulle få exakt samma utformning på frågorna och information inför testet. Instruktionerna och uppgifterna för användartestet finns i Bilaga 1

Målgruppen för användartestet var personer med kunskap inom cybersäkerhet och som nyttjar Lore i dagsläget eller har intresse att använda verktyget i framtiden. Alla personer som tillfrågades om att delta i användartestet var forskare eller forskningsingenjörer på FOI på enheten för informationssäkerhet och IT-arkitektur, som på ett eller annat sätt medverkar i cybersäkerhetskurser eller -övningar. För att testa hur intuitivt användargränssnittet var tillfrågades personer med varierande erfarenheter inom Lore, samt olika roller inom cybersäkerhetsövningar som exempelvis rött lag, övningsledare, observatörer och personer som ansvarar för infrastruktur under övningar. Alla deltagare blev inbjudna via mail med en kort beskrivning av testet. Totalt bokades sex separata användartester in utspritt över tre veckor där varje användartest planerades att pågå i en timme.

Samtliga användartester utfördes i en lokal vid FOI i Linköping. Testet började med att testdeltagarna fick svara muntligt på ett antal frågor angående Lore och Lore GUI, därefter presenterades instruktionerna och uppgifterna i form av ett utskrivet papper. Testdeltagarna fick läsa instruktionerna i lugn och ro innan de påbörjade uppgifterna. Under användartestets genomförande uppmanades deltagarna att tänka högt och kommentera hur de löste uppgifterna. Deras kommentarer, lösningssätt och tid att lösa uppgifterna dokumenterades. Tiden dokumenterades framför allt för att se den tidsmässiga skillnaden mellan deltagare med olika roller och förkunskap inom Lore. När alla uppgifter hade utförts fick deltagaren besvara ett antal frågor angående testets genomförande. Samtliga frågor som framfördes före och efter uppgifterna finns i Bilaga 2. En sammanställning av samtliga användartester finns i kapitel 4.

4 Resultat av användartesterna

I det här kapitlet presenteras en sammanställning av resultaten för samtliga användartester om hur intuitivt Lore GUI är för teknisk informationshämtning. Tabell 1 beskriver testdeltagarnas svar på frågorna som ställdes innan uppgifterna presenterades, där frågorna fokuserade på testdeltagarnas förkunskaper om bland annat Lore och Lore GUI.

Tabell 1: Frågor och svar om testdeltagarnas förkunskaper om Lore och Lore GUI. TD = Testdeltagare.

Fråga	TD 1	TD 2	TD 3	TD 4	TD 5	TD 6
Har du använt Lore GUI innan?	Ja	Ja	Ja	Nej	Nej	Nej
Har du använt Lore innan?	(Ja) Begränsat.	Ja	Nej	Nej	Nej	Nej
Medverkade du i Safe cyber 2022? Vilken roll hade du i så fall?	Nej, men medverkat tidigare år som övningsledare	Ja, rött lag	Nej, men medverkat tidigare som rött lag	Ja, observatör	Ja, övningsledare	Ja, ansvarade för infrastruktur
Hur ofta använder du verktyg dom utför olika typer av angrepp? (t.ex. serverangrepp, kartläggning, osv)	Aldrig	Dagligen	Ibland, vid övningar	Nästan aldrig	Väldigt sällan	Väldigt sällan

I Tabell 2 beskrivs samtliga testdeltagares resultat på alla uppgifter under användartesterna, samt den totala tiden det tog för varje testdeltagare att utföra alla uppgifter.

Tabell 2: Resultat av uppgifterna under användartestet. R = Uppgift utförd korrekt, R* = Uppgift utförd korrekt efter hjälp, F = Uppgift inte avklarad eller fel slutsats.

Uppgift	TD 1	TD 2	TD 3	TD 4	TD 5	TD 6
1	R	R	R	R	R	R
2	R	R	R	R	R	R
3	R	R	R	R	R	R
4.1	R	R	R	R	R*	R
4.1.1	R	R	R	R	R	R
4.1.2	R*	R	R*	R	R	R
4.2	R	R	R	R	R	R
4.2.1	R	R	R	R	R	R
4.2.2	R	R	R	R	R	R
4.2.3	R	R	R	R	R	R
4.3	R	R	R	R	R	R
4.3.1	R	R	F	R	F	R
4.3.2	R	R	R	R	R	R
4.4	R	R	R	R	R	R
4.4.1	R	R	R*	R	R	F
5.1	R	R	R	R	R	R
5.2	R	R	R	R	R	R
5.3	R	R	R	R	R	R
5.3.1	F	R	R	R	R	F
5.3.2	R	R	R	R	R	R
Total tid	23:06	15:51	28:43	24:55	25:41	23:27

Av frågorna som ställdes efter uppgifternas utförande framgick det att de testdeltagarana som använder Lore ansåg att Lore GUI har potential att hjälpa dem i deras arbetsuppgifter. De testdeltagarna som inte använder Lore för tillfället ansåg att Lore GUI skulle kunna hjälpa dem att börja använda Lore vid behov. Dessutom var det ingen av testdeltagarna som ansåg att det saknades

funktionalitet eller information för att lösa de uppgifter som gavs under testet. Dock förmedlade testdeltagarna konstruktiv kritik och förbättringsförslag om vad de tyckte kunde göra användargränssnittet mer intuitivt.

5 Slutsatser och diskussion

Memot beskriver ett användartest som har utförts på användargränssnittet, kallat Lore GUI, för verktyget Lore. Användartestet utfördes för att testa hur intuitivt användargränssnittet var för teknisk informationshämtning vid förberedelser, initiering och tolkning av resultat från scenarier. Användartestet genomfördes i form av frågor och uppgifter som skulle spegla vanliga arbetsuppgifter en operatör i användargränssnittet skulle kunna ha. Testdeltagarana var forskare och forskningsingenjörer från FOI på enheten för informationssäkerhet och IT-arkitektur och hade olika roller i cybersäkerhetsövningar samt varierad erfarenheter om Lore och Lore GUI.

Resultatet visar att en stark majoritet av uppgifterna gick att utföra korrekt utan någon hjälp oavsett roll och erfarenhet i Lore och Lore GUI. Därför anses användargränssnittet vara tillräckligt intuitivt för en oerfaren operatör att utföra vanliga uppgifter i Lore GUI utan extern hjälp, dock finns det förbättringspotential att göra användargränssnittet mer intuitivt. Dessutom visas att tiden det tog att lösa uppgifterna för en testdeltagare med erfarenhet av Lore var märkbart kortare jämfört med testdeltagare utan erfarenhet. Däremot var det ingen märkbar tidsskillnad på testdeltagare med eller utan erfarenhet av användargränssnittet. Tidsåtgången är dock otillförlitlig som jämförelseaspekt eftersom testdeltagarna uppmanades att inte utföra uppgifterna så snabbt som möjligt. Dessutom korrelerar inte tiden det tog att utföra uppgifterna med antalet rätt utförda uppgifter. Däremot kan tidsåtgången ge en indikation på hur lång tid det tar för en användare att förstå informationen i det grafiska gränssnittet, vilket påverkas av hur intuitivt användargränssnittet är.

6 Referenser

[1] H. Holm, ”Automatisering av cybersäkerhetsövningar – Vidareutveckling och evaluering av Lores beslutsprocess,” Linköping, 2021.

Bilaga 1: Instruktioner och uppgifter för användartest av Lore GUI

Tack för att du vill vara med på användartest för användargränssnittet, Lore GUI! Användartestet kommer gå ut på att utföra ett antal uppgifter med hjälp av användargränssnittet samt besvara ett antal frågor kopplade till Lore och Lore GUI. Efter användartestet kommer ytterligare några frågor ställas angående användargränssnittet.

Uppgifterna är utformade för att testa hur intuitivt Lore GUI är för att förstå teknisk information när man ska skapa, redigera och starta scenarion samt tolka scenarios loggar och resultat. **Användartestet är till för att undersöka användargränssnittet, inte dig**. Utför alla uppgifter i nummerordning. Om du tycker att några av frågorna är för svåra att förstå eller lösa så är det helt okej att hoppa över dem, men försök gärna lösa uppgifterna även om de känns svåra.

Uppgifterna kommer att gå på tid. Detta är till för att se vilka av uppgifterna som användarna kan fastna på eller vara svåra att lösa, så jag vill inte att du ska försöka att utföra frågorna så snabbt som möjligt, gör dem i normal takt.

När du utför uppgifterna så vill jag att du tänker högt, t.ex. hur du ska försöka lösa uppgiften, hur du navigerar i användargränssnittet, och vad som är svårt eller lätt att förstå. Berätta även när du påbörjar en ny uppgift samt när du känner dig klar med en uppgift. Du behöver inte skriva ner dina svar för uppgifterna, det räcker att du säger svaren/lösningen högt.

Under tidens gång kommer jag att anteckna hur du löser uppgifterna, om du hoppar över några uppgifter, vilka svar du kom fram till och om du har några andra tankar eller åsikter. Jag kommer inte säga om dina svar är rätt eller fel och kommer inte att hjälpa dig att lösa uppgifterna om du inte explicit ber om hjälp. Ifall ditt svar kommer påverka efterkommande frågor så kommer jag eventuellt rätta dig och berätta det rätta svaret.

Har du några frågor under testets gång så är det bara att fråga.

Om du har några frågor innan användartestet startar så kan du fråga dem nu.

Om du känner dig redo så kan du säga det högt och påbörja testet genom att vända blad och börja på uppgift 1. Så fort du vänder blad startar tidtagningen. Lycka till!

Uppgifter

1. Skapa ett scenario

Skapa ett scenario (använd ”Simple Form”) med namnet(label) ”**Safe Cyber user test**” med följande specifikationer:

- Välj den röda profilen till: SAFE Cyber 2022 (NORTH) (id: 53).
- Svartlista adresserna 11.101.0.0/16 och 11.102.0.0/16.
- Välj Crate miljön(environment) till Safe Cyber 2022 som ligger i FM-zonen.
- Välj en valfri injektor och sätt ett VXLAN den ska börja på. Välj ett VXLAN från segment-listan i den förberedda coreweb -fliken.
- Lägg till så att det finns förkunskap om nätverkssegmenten 66.88.0.0/24 och 72.27.4.0/24.

2. Editera ett scenario

Editera ”**Safe Cyber user test**” efter följande specifikationer:

- Skapa ett nytt mål för scenariot med namnet(label) *deface www* som går ut på att ta över maskinen med IP 66.88.32.12 med system rättigheter samt ett skal (bakdörr) av typen meterpreter.
- Justera prioriteringar och sätt så att nätverkssegmentet med IP 72.72.4.20 ger 100 gånger mer poäng ifall kompromitterad.

3. Starta ett scenario

Gå tillbaka till scenariovyn och starta **Safe Cyber user test**. Efter att scenariot har startat, stoppa scenariot.

4. Tolka utfall av ett scenario

Förstå resultatet av scenariot CYBON Scenario 1 (id: 73), genom att gå in i instansen ”**CYBON Scenario 1 session 5** (id: 139)” för att visa instansens red team knowledge och utför nedanstående uppgifter.

4.1. Visa maskiner i tabellen.
- **4.1.1.** Hur många maskiner har hittats av Lore?
- **4.1.2.** Hur många maskiner hade hittats av Lore t.o.m. kl. 09:57:10?

4.2. Leta rätt på maskin: **152.61.3.15.**
- **4.2.1.** Hur många döda och aktiva skal(bakdörrar) finns på maskinen?
- **4.2.2.** Har maskinen blivit kompromettерad? Om ja; vilken aktion användes för att skapa ett skal på maskinen och vad gjorde den? (Hint: dubbelklicka för mer information)
- **4.2.3.** Finns det några kända konton på maskinen **152.61.3.15?** Om ja; Vad har kontot/kontona för användarnamn och lösenord? (Hint: dubbelklicka för mer information)

4.3. Gå tillbaka till tabellen och leta rätt på maskin **152.61.3.27**.
- **4.3.1.** Hur många aktioner har körts mot maskinen?
- **4.3.2.** En av aktionerna som har körts på maskinen är ”*post/windows/manage/archmigrate*”. Den har en inställning som heter SESSION, vad är SESSION-parametern satt till i den aktionen?

4.4. Gå tillbaka till tabellen och visa nätverkssegment istället för maskiner. Markera samtliga nätverkssegment och visa ”force directed graph”. I *additonal info* ovanför grafen markera ”shell”, därefter rendera grafen.
- **4.4.1.** Med hjälp av grafen; hur många nätverkssegment innehåller kompromettерade maskiner.

5. Tolka mål av ett scenario

Gå tillbaka till listan över scenarion och gå samma instans (**CYBON Scenario 1 session 5** i CYBON Scenario 1 (id: 73)) och gå vidare till ”Goals” för att se status på de mål som var uppsatta för scenariot och utför nedanstående uppgifter.

5.1. Hur många mål blev avklarade?

5.2. Hur många blev inte avklarade?

5.3. Vilket mål blev avklarat först?
- **5.3.1.** Vilka aktioner kördes efter att det målet avklarades?
- **5.3.2.** En av aktionerna som kördes var *CecStatusReport*. Vad gör den aktionen?

Bilaga 2: Frågor inför/efter användartest Lore GUI

Frågor inför användartestet

- Har du använt Lore GUI innan? Om ja: till vad?
- Har du använt Lore innan?
- Medverkade du i Safe cyber 2022?
    - Om ja: Vilken roll hade du då?
    - Om nej: Har du medverkat i någon annan övning? Vad hade du för roll då?
- Hur ofta använder du verktyg som utför olika typer av angrepp som Lore använder? (t.ex serverangrepp, kartläggning, osv)

Frågor efter användartestet

- Tror du att detta användargränssnitt skulle kunna underlätta dig i några av dina arbetsuppgifter?
- Var det något du saknade för att lösa de uppgifter som gavs?
- Var det något du saknade i användargränssnittet som du förväntade dig?