Laboration Felsökning - Windows Tredjepartsverktyg

Översiktliga labbinstruktioner för felsökning Windows Loggboken.

Material: Man behöver tillgång till en Windows 10/11 dator (eller VM) samt ha lokal administratörsbehörighet till operativsystemet.

Laboration 1: Använda Sysinternals Process Explorer och Process Monitor

Mål

Lära sig att använda Process Explorer och Process Monitor för att övervaka och felsöka processer och systemaktiviteter i Windows.

Förberedelser

1. Ladda ner och installera Process Explorer från Sysinternals.
2. Ladda ner och installera Process Monitor från Sysinternals.

Steg

1. **Starta Process Explorer**:
    - Öppna Process Explorer.
    - Utforska gränssnittet och identifiera de olika sektionerna (processlista, detaljerad information om en vald process, etc.).
    - Välj en process (t.ex. explorer.exe) och undersök dess detaljer (CPU-användning, minnesanvändning, trådar, etc.).
2. **Analysera en process**:
    - Högerklicka på en process och välj “Properties”.
    - Gå igenom flikarna (Image, Performance, Threads, TCP/IP, etc.) och notera viktig information om processen.
3. **Starta Process Monitor**:
    - Öppna Process Monitor.
    - Bekanta dig med gränssnittet och de olika filtreringsalternativen.
4. **Övervaka systemaktiviteter**:
    - Starta en ny övervakningssession genom att klicka på “Capture” (Ctrl+E).
    - Utför en specifik åtgärd på datorn (t.ex. öppna en fil eller starta ett program) och observera hur Process Monitor registrerar händelserna.

   - Använd filtreringsfunktionen för att begränsa visningen till specifika händelser (t.ex. filsystemaktivitet eller registerändringar).

5. **Analysera loggar**:
   - Stoppa övervakningen (Ctrl+E).
   - Gå igenom loggarna och identifiera viktiga händelser relaterade till den åtgärd du utförde.
   - Exportera loggarna till en fil för vidare analys.

Reflektion

- Vad lärde du dig om de processer och systemaktiviteter du övervakade?
- Hur kan dessa verktyg användas för att felsöka specifika problem i Windows?

Laboration 2: Använda NirSoft Wireless Network Watcher och ProduKey

Mål

Lära sig att använda Wireless Network Watcher för att övervaka nätverksanslutningar och ProduKey för att återställa produktnycklar.

Förberedelser

1. Ladda ner och installera Wireless Network Watcher från NirSoft.
2. Ladda ner och installera ProduKey från NirSoft.

Steg

1. **Starta Wireless Network Watcher**:
   - Öppna Wireless Network Watcher.
   - Bekanta dig med gränssnittet och de olika alternativen.
2. **Övervaka nätverksanslutningar**:
   - Starta en skanning av ditt nätverk genom att klicka på “Start Scanning” (F5).
   - Identifiera alla enheter som är anslutna till ditt nätverk.
   - Notera viktig information om varje enhet (IP-adress, MAC-adress, enhetsnamn, etc.).
3. **Analysera nätverksaktivitet**:
   - Identifiera eventuella okända eller misstänkta enheter.
   - Exportera listan över anslutna enheter till en fil för vidare analys.
4. **Starta ProduKey**:
   - Öppna ProduKey.
   - Bekanta dig med gränssnittet och de olika alternativen.
5. **Återställa produktnycklar**:

- Använd ProduKey för att återställa produktnycklar för installerade program och operativsystem.
- Notera de återställda nycklarna och spara dem på en säker plats.

Reflektion

- Hur kan Wireless Network Watcher användas för att förbättra nätverkssäkerheten?
- Hur kan ProduKey vara användbart vid återställning av system eller programvaror?

Laboration 3: Använda Hirens Boot CD för felsökning

Mål

Lära sig att ladda ner, skapa en bootbar enhet och starta upp Hirens Boot CD för att använda dess verktyg för felsökning och reparation av en dator.

Förberedelser

1. En dator med internetuppkoppling.
2. En tom USB-enhet (minst 2 GB).
3. Programvara för att skapa en bootbar USB-enhet (t.ex. Rufus).

Steg

1. **Ladda ner Hirens Boot CD**:
   - Gå till Hirens Boot CD:s officiella webbplats.
   - Ladda ner den senaste ISO-filen.
2. **Skapa en bootbar USB-enhet**:
   - Ladda ner och installera Rufus från Rufus officiella webbplats. (eller använd winget)
   - Anslut USB-enheten till datorn.
   - Öppna Rufus och välj din USB-enhet under “Device”.
   - Klicka på “SELECT” och välj den nedladdade Hirens Boot CD ISO-filen.
   - Under “Partition scheme”, välj “MBR” om du ska använda enheten på en äldre dator eller “GPT” för nyare datorer.
   - Klicka på “START” för att börja skapa den bootbara USB-enheten.
3. **Starta upp från USB-enheten**:
   - När USB-enheten är klar, starta om datorn.
   - Gå in i BIOS/UEFI-inställningarna (vanligtvis genom att trycka på en tangent som F2, F12, DEL eller ESC under uppstart).
   - Ändra startordningen så att datorn startar från USB-enheten först.

- Spara ändringarna och starta om datorn.

4. **Använda Hirens Boot CD**:
    - När datorn startar från USB-enheten, kommer Hirens Boot CD att starta.
    - När operativsystemet har laddats, utforska de olika verktygen som finns tillgängliga för felsökning och reparation.
    - Använd verktyg som “Check Disk”, “Registry Editor”, “Password Reset” och andra för att lösa eventuella problem med datorn.

Reflektion

- Vilka verktyg på Hirens Boot CD fann du mest användbara och varför?
- Hur kan Hirens Boot CD hjälpa till vid allvarliga systemproblem som inte kan lösas från det vanliga operativsystemet?