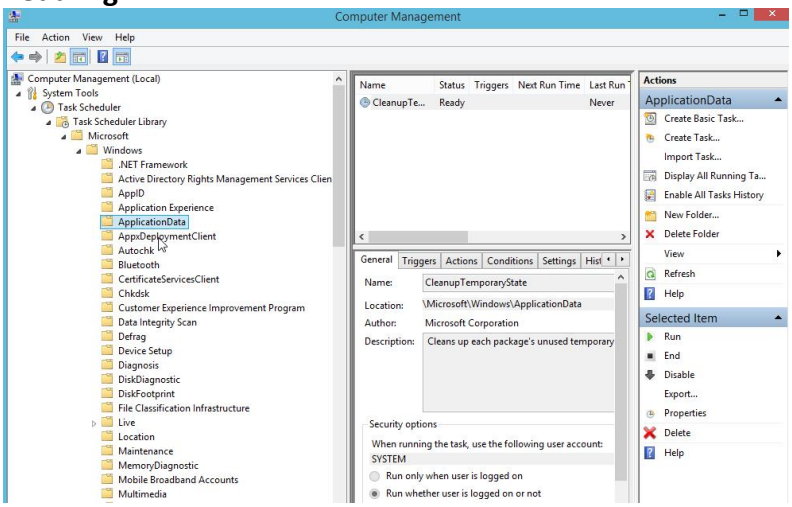
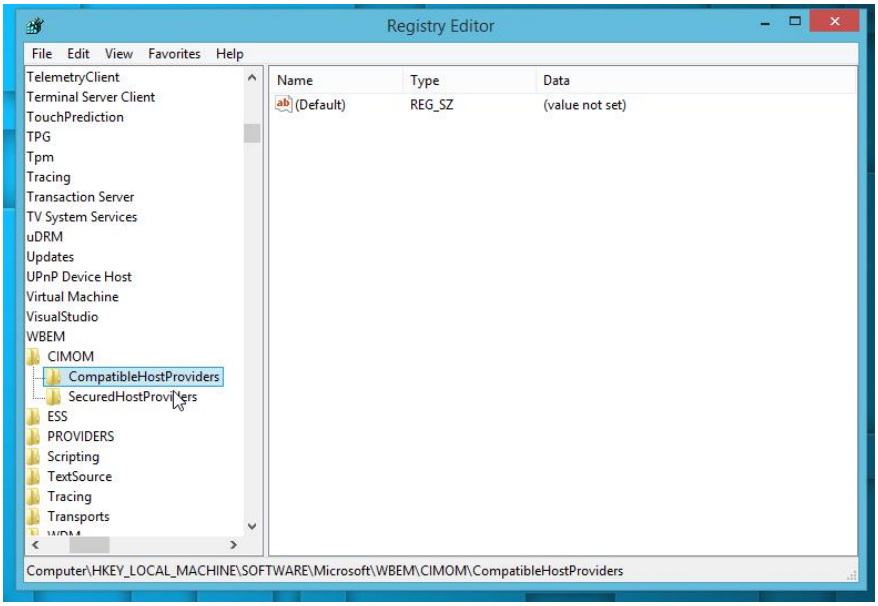
**Laboratorul 1**
**Auditare stație de lucru cu MS Windows**

Auditările de securitate pentru un sistem de operare pot fi interne sau externe și pot fi realizate continuu sau asincron. SE va folosi mașina virtuală disponibilă pe stație pentru a instala și testa fiecare din instrumentele care vor fi prezentate mai jos.
În acest laborator ne vom axa pe analiza instrumentelor care pot fi folosite pentru auditări interne de securitate
1. Analiza setărilor de securitate aflate în registrul intern al Windows-ului. (msconfig)
Realizati si comparati analiza conexiunilor active cu tcpview sau netstat (testati si Microsoft Network Monitor, GlassWire si Wireshark )
2. Analiza antivirus
3. IDS-uri

**Windows Scheduling**




Permite optimizare de performante dar și urmărirea stării unor aplicații directe sau colaterale care urmăresc diverse aspecte din sistem
Cu regedit se pot verifica/analiza/verifica majoritatea cheilor și setărilor utilizate de Windows. Aici se fac adăugiri și sau modificări de către multe aplicații nedorite.




**Intrusion Detection Systems - IDS suportate și de Windows**

**1. Snort**

Este un utilitar furnizat de CISCO, din categoria "oldest but goldest" care poate fi instalat atât pe Windows cât și pe linux. Deși este ușor depășit în comparație cu Suricata care prezintă o serie de avantaje este încă o prezentă demnă de luat în considerare atât din punct de vedere a ultimilor îmbunătățiri care i-au dat un nou suflu cât și datorită unei baze de cunoștințe destul de mare la nivelul experienței utilizatorilor în utilizarea lui. Pentru multă lume abilitățile lui nu pot fi utilizate complet deoarece necesită pentru aceasta cunoașterea limbajului Ruby. La instalarea pe Windows acesta va solicita și instalarea lui WinPcap deoarece este necesar pentru a putea realiza o monitorizarea completă a traficului de rețea.

În Windows se va instala în directorul implicit snort pe discul C dacă altă cale nu este furnizată. Poate fi lansat din subdirectorul *bin*. Deoarece inițial a fost numai pentru Linux interacțiunea este tot de tip consolă și dat fiind și observațiile anterioare rămâne recomandat numai pentru utilizatorii care au cunoștințe decente în domeniul securității informațiilor. Acesta permite și dezvoltarea de detectoare particularizate utilizând Lua-c ceea ce îl va menține probabil încă multă vreme activ pe piață.

**2. OSSEC**

Un alt IDS gratuit și "open source" care a fost gândit pentru servere dar permite instalarea unui client și pe o mașină Windows. Este bazat pe conceptul de log-based IDS și ne permite dezvoltarea de aplicații particularizate care să analizeze jurnalele generate de acesta. Ne permite de asemenea și verificare integrității fișierelor atât pe linux cât și pe Windows, verificarea registry-ului pentru Windows dar și și analize de rootkit pentru linux sau chiar contra acțiuni dacă este configurat/programat corespunzător.

Suportă o mare varietate de plugin-uri care în cazul IDS-urilor sunt denumite decodoare (decoders). La nivel client în afara monitorizării traficului de rețea va genera alerte (prin monitorizarea log-urilor) cu privire la poșta electronică sau activitatea discutabilă a unor executabile active în sistem. Dezvoltarea de decodoare

personalizate este realizată cu ajutorul unor fișiere XML dar necesită inclusiv cunoștințe de utilizarea a regex-ului pentru analize mai complicate a fișierelor de jurnalizare.

**3. Suricata**

Poate fi văzut ca succesorul Snort dar cu o serie de abilități pe care acesta încă nu le-a dobândit. Mai mult nivelul de integrare nativă cu serviciile și tool-urile de tip cloud este nativă ceea ce îi dă un mare avantaj în fața acestuia. Din nefericire fiind relativ nou suportul oferit de comunitate este relativ scăzut și atunci pentru mulți administratori utilizarea lui este relativ limitată la utilizarea consolă sau a componentelor suplimentare care permit o gestionare vizuală. Aceste lucruri nu îi diminuează valoarea curentă dar face greoaie dezvoltarea de instrumente mai particularizate pentru necesitățile utilizatorului. Este orientat pe monitorizarea rețelei dar nivelul de reactivitate la atacuri pe care ăl posedă este superior snort-ului. Este din categoria “real time intrusion detection”, “inline intrusion detection”, “network monitoring” dar și “pcap processing”. Pentru detectarea unor amenințări mai complexe există un suport pentru script-uri Lua. Datorită faptului că utilizează YAML și JSON pentru fișierele de intrare și ieșire este compatibilă cu instrumente cum ar fi SIEMs, Splunk, Logstash/Elasticsearch, Kibana, precum și alte baze de date.

**4. Zeek Network Security Monitor**

Inițial era denumit Bro și a rămas un software gratuit sub licență BSD. Acesta are o abordare ușor diferită față de IDS-urile standard. O abilitate constă în aceea că a fost construit pentru flexibilitate maximă. Ca rezultat el va permite, cu ajutorul unor limbaje de tip script care sunt specifice în funcție de domeniu, dezvoltarea de module care permite monitorizarea particularizată pentru fiecare site aflat sub control. El este dedicat pentru gestiunea rețelelor și site-urilor de mare performanță și încărcare. Nu se bazează pe abordări clasice cu privire la seturi de semnături sau pe anumite scheme de detecție standard. Rezultă că nici acesta nu este recomandat utilizatorilor medii. Ca și în cazul anterior furnizează jurnale detailate cu privire la activitățile din rețea permițându-ne totodată analize semantice de nivel superior asupra acestora prin intermediul modulelor dedicate puse la dispoziție. De asemenea monitorizează extensiv nivelul aplicației din modelul ISO-OSI. A fost gândit cu interfețe deschise ceea ce permite interoperabilitate aproape nelimitată inclusiv schimb în timp real de informații cu alte aplicații de profil.

**5. Sagan**

Este un instrument de monitorizarea jurnalelor care poate integra date generate de snort.

Următoarele nu mai necesită prezentări deosebite:

- **Comodo**
- **Kaspersky Total Security 2018**
- **Cylance Smart Antivirus**
- **Trend Micro Business Solution**
- **Norton Internet Security**

**Temă de laborator**

Utilizati nat in configurarea manierei de legare in retea

În mașina minimală de Windows 8 disponibilă instalați testați și eventual configurați utilitarele prezentate anterior.

**Temă pe acasă**

Reluați aceste teste pe laptop-ul personal și realizați un raport despre comportamentul lui pentru fiecare aplicație din laborator (în termeni de încărcare suplimentară indusă asupra sistemului - un tabel comparativ urmărind memorie, procesor, handle fișiere, memorie virtuală etc). În raport se vor specifica și caracteristicile hardware/software ale sistemului utilizat pentru testări.