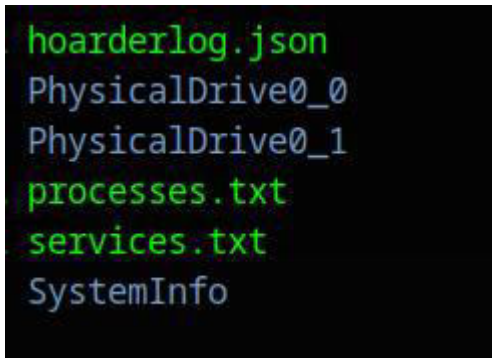
log-analysis1

Here we go avemun challenge de forensics aici mai ales un zip care contine informatii legate de procese,comenzi,fisiere etc.. care se aflau pe masina atacata.



Q1. What is the full command used to dump the lsass process on the targeted system?

La astfel de intrebari merg direct la comenzi care au fost folosite in powershell / command prompt.Daca ne ducem in PhysicalDrive0_0 o sa vedem un director care contine PowerShellHistory ceea ce cautam noi mai exact urmand acest fisier pana la fisierul text care contine fiecare comanda powershell unde stim (din desciere) ca a folosit procesul lsass pentru a da dump la toate parolele de pe sistem:

grep -E lsass ConsoleHost_history.txt

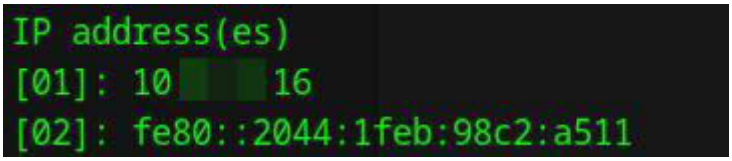
Vedem mai multe comenzi care contin processul lsas + procdump.exe(Rulează **ProcDump**, un instrument oficial de la Microsoft (din Sysinternals Suite), folosit pentru a crea dump-uri de memorie ale proceselor)

Raspuns:

Q2. What is the IP address of the compromised computer? (Points: 100)

Pentru a raspunde la aceasta intrebare vom folosi SytemInformation si in fisierul Output.txt vedem raspunsul sub IP adress(es).

Raspuns:



Q3. What is the command used by the attacker to enumerate all system users? (Points: 100)

Tot ca la Q1 ma duc in fisierul de comenzi executate in powershell.Aici ma gandeam la comenzi de tip net folosite.Comanda **`net`** în Windows este un utilitar din linia de comandă, folosit pentru a

administra utilizatorii, grupurile și alte resurse de rețea. Când vine vorba de **gestionarea utilizatorilor**, `net` oferă funcționalități esențiale pentru administratori, permițându-le să adauge, să modifice și să elimine conturi de utilizator și să gestioneze grupurile de securitate locale.Deci folosim comanda : **grep -e net ConsoleHost_history.txt**

Raspuns:

```
└──╼ $grep -e net ConsoleHost_history.txt
http://blogs.technet.com/b/heyscriptingguy/archive/2012/07/05/use-powershell-to-duplicate-process-tokens-via-p-invoke.aspx`
http://www.labofapenetrationtester.com/2015/09/bypassing-uac-with-powershell.html`
net localgroup users
net
```

Q4. Which MITRE technique can be assigned to a case where OS passwords are dumped? Flag format <technique_ID>:<technique_name> (Points: 100)

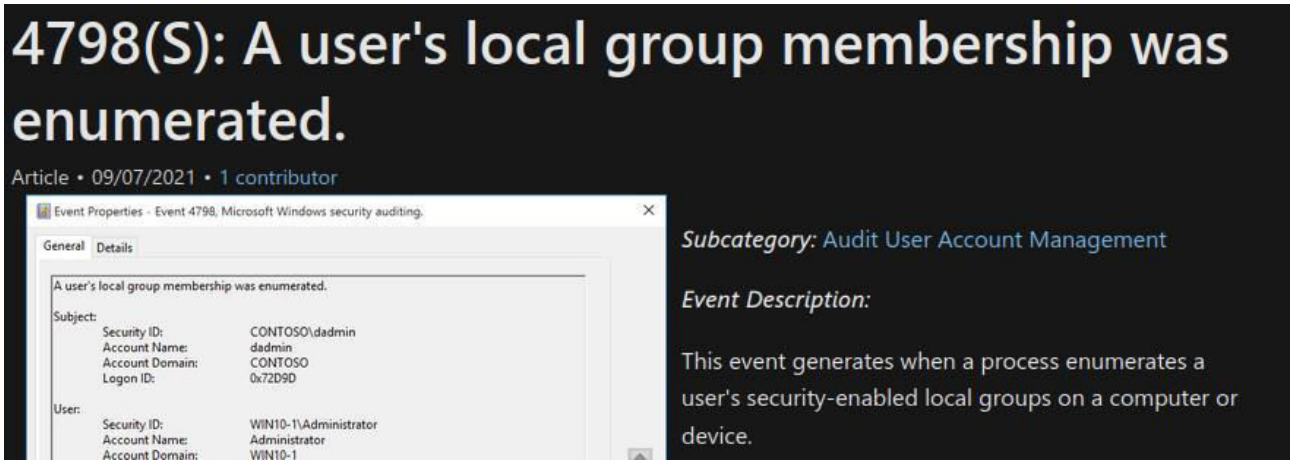
Aici mai multe este osint pentru a gasi id .Am cautat pe google MITRE technique os password dump si a am gasit printre primele raspunsuri:

Raspuns:

T1003:…..

Q5. Which Windows Security event code was triggered when the attacker attempted to enumerate the existing local groups on the compromised system? (Points: 100)

In windows exista fisiere specifice pentru a documenta tot ce se intampla pe o masina gazda.Fișierele **.evtx** sunt fișiere de jurnal de evenimente (event log) folosite de Windows pentru a stoca înregistrări detaliate despre activitatea sistemului, a utilizatorilor și a aplicațiilor. De obicei se gasesc in C:\Windows\System32\winevt\Logs\ printre acestea avem si **`Security.evtx`** care este unul dintre cele mai importante fișiere pentru analiza criminalistică (forensics) și securitate cibernetică. Acesta înregistrează toate evenimentele de securitate configurate în politica locală de audit.Putem gasi acest tip de fisiere aici in phisical drive 0 Events/Windows/System32/winevt/Logs iar toolul pe care l-am folosit sa vad fisierul Security.evtx din cli este evtxexport .Am cautat aici putin si pe google care este codul tipic pentru asta si am gasit .



Dupa asta ca sa confirm suspiciunea am folosit : **evtxexport Security.evtx | grep 4798** Raspuns:Mai evident de atat nu se poate

Trolled by masquerade8077