***PE Blue Team: Autopsy (1ster)***

Task1

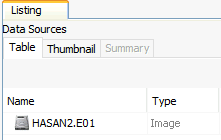
1.1:

We hebben de autopsy file ingeladen die in de map “Case Files” stond.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Na het inladen krijgen we een .E01 image file te zien.



Na het selecteren van dit bestand kan je onderaan “File Metadata” selecteren waar de MD5 te zien is.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1.2:

Op locatie Results\Extracted Content\Operating System Information hebben we de informatie van het systeem gevonden met de computer name.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1.3:

Op locatie Results\Extreacted Content\Operating System User Account hebben we de informatie van de user accounts.

Hier hebben we software-, administrator-, guest-, default accounts niet genomen maar enkel de gebruikersnamen.

Afbeelding met tafel

Automatisch gegenereerde beschrijving

1.4:

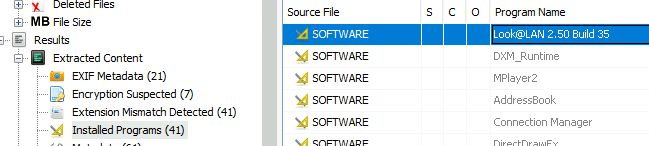
Op locatie Results\Extreacted Content\Operating System User Account hebben we de informatie van de user accounts en onder de kolom “Data Accessed” kunnen we zien wanneer dit account het laatst is ingelogd.

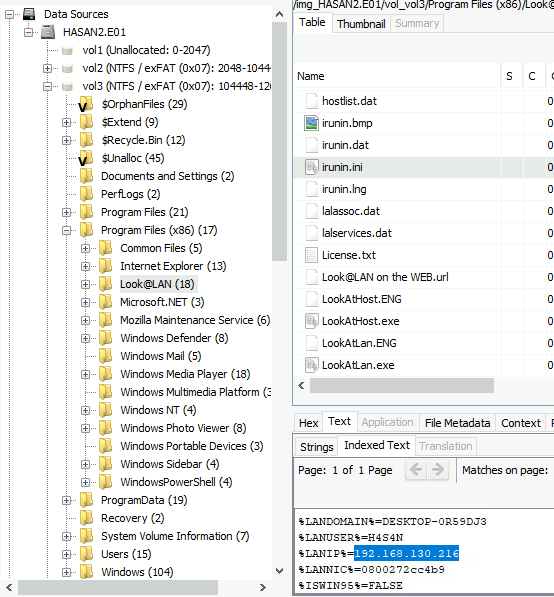
Afbeelding met tekst

Automatisch gegenereerde beschrijving

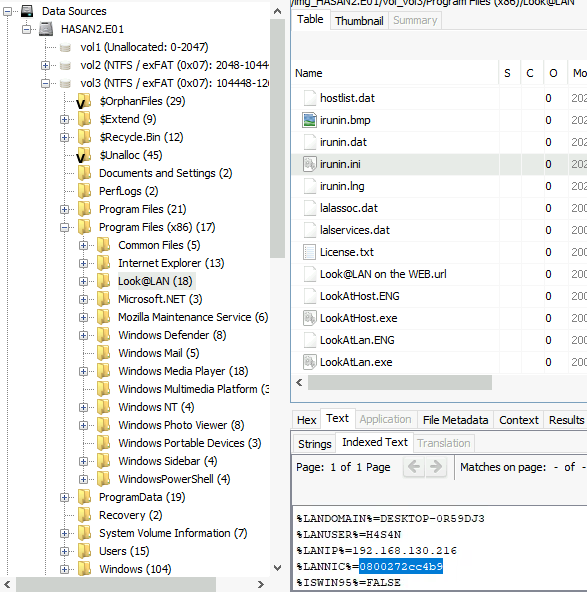
1.5:

Op locatie Op locatie Results\Extreacted Content\Installed Programs vinden we een network monitoring tool (Look@lan). Nu gaan we in “Data Sources” kijken of we dit programma terugvinden in “Program Files”. Dit hebben we teruggevonden in “vol3”. In de logfile “irunin.ini” vinden we de log bestanden met hierin “LANIP” wat ons IP address is.





1.6:

In dezelfde file die we gebruikt hebben in de vorige vraag vinden we ook “LANNIC” wat ons MAC address is van de computer.  


1.7:

De network card details hebben we gevonden door naar het keyword “ethernet” te zoeken en als we door de files gingen hebben we onder DiagnosticLogCSP\_Collector\_DeviceProvisioning…. de ethernet adapter gevonden.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1.8:

Dit bestand hadden we nodig om vraag 1.5 en 1.6 op te kunnen lossen. En het network monitoring tool was Look@Lan.

1.9:

We moeten een “Bookmark” zoeken. We zien in Autopsy dat er een folder staat “Web Bookmarks”. Als we hierop klikken kunnen we in de details een bookmark voor Google Maps vinden met de coördinaten.

Afbeelding met tekst

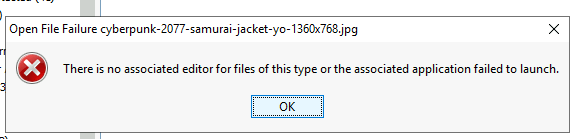
Automatisch gegenereerde beschrijving

1.10:

In Autopsy hebben we een menu “Images/Videos”. Als we hierop klikken kunnen we van elke user hun afbeeldingen bekijken. We hebben elke afbeelding bij elke user bekeken tot we bij Joshwa zijn naam hebben gezien op een van de afbeeldingen.

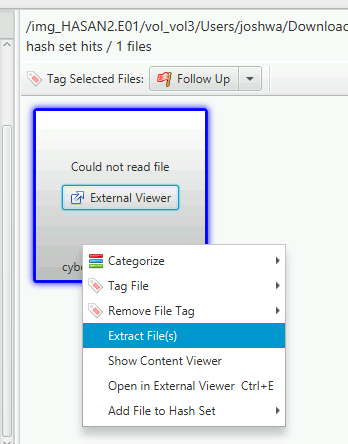
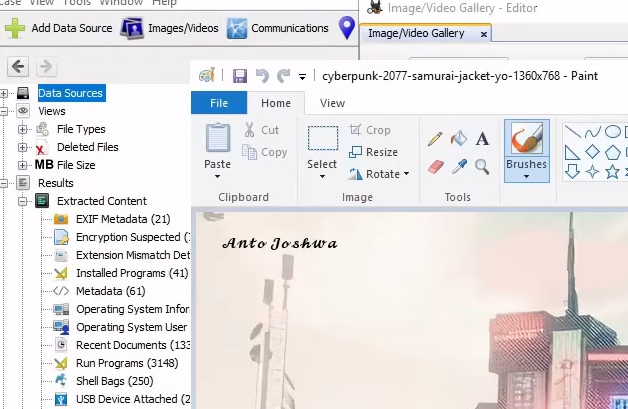
Probleem:

1. We konden de afbeeldingen niet openingen in Images viewer



Oplossing:

1. We konden de afbeelding extracten en dan zo openen in paint.



1.11:

Als we een aangepaste file moeten zoeken denken we onmiddellijk aan logs. Ook het programma “powershell” is gebruikt.

Probleem:

1. Waar staan deze logfiles?

Oplossing:

1. Na opzoekwerk vonden we dat als de gebruiker powershell heeft gebruikt, dit terug te vinden was op volgende locatie: \user\AppData\Roaming\Microsoft\Windows\Powershell.

We zijn dan bij elke user gaan kijken of we logfiles konden vinden die horen bij “Powershell”. We hebben een txt bestand gevonden bij Shreya in de folder “PSReadLine” onder “Powershell”. Dit bestand hebben we geselecteerd en in de meta data hebben we onder cd .\Desktop\ de eerste gegevens “Add-Content” gevonden. Dit heeft ons doen vermoeden dat dit de eerste flag van het bestand was.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1.12:

Probleem:

1. Waar vinden we de exploit?
2. We moeten een boodschap in de vorm van een “flag{}” vinden.

Oplossing:

1. Via keyword gezocht op exploit maar niet gevonden wat we zochten.
2. Via keyword gezocht op flag om te kijken of dit een resultaat opleverde.

Hier hebben in de resultaten een mapje exploit gevonden waarin we de gevraagde flag hebben gevonden.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1.13:

Probleem:

1. Welke tools worden gebruikt om paswoorden te vinden in een systeem?
2. Waar kunnen we deze tools vinden?

Oplossing:

1. Googelt welke tools dit zouden kunnen zijn maar zonder duidelijk resultaat.
2. In autopsy hebben we een mapje “run programs” gevonden. Dit gaf alle gestarte programma’s weer. Als je al deze resultaten op “username” sorteert zie je in de resultaten username “H4S4N” terugkomen. Dit is dezelfde naam als de “Data Source” die we te zien kregen na het inladen van de autopsy file.

Na de sortering hebben we eens gekeken welke soorten “program names” gestart werden bij deze user. We hebben alle voor ons onbekende programma namen genoteerd en dan in google gekeken waarvoor deze programma’s dienen. Hieruit hebben we 2 resultaten gevonden -> Mimikatz en Lazagne. Tools gebruikt om authenticatie gegevens op te zoeken (paswoorden en usernames).

Afbeelding met tekst, schermafbeelding, zwart, scherm

Automatisch gegenereerde beschrijvingAfbeelding met tekst, schermafbeelding, monitor, zwart

Automatisch gegenereerde beschrijving

1.14:

Probleem:

1. Wat is een “Yara” file?
2. Waar kunnen we dit vinden?

Oplossing:

1. Gegoogeld wat dit is: Yara is een tool dat vooral gebruikt wordt voor malware research and detection. Het baseert zich op regels die bestaan uit strings en boolean expressies. En wordt weergegeven als een .yar file.
2. Geen idee, we hebben geprobeerd door in “search keyword” .yar in te geven en gekeken welke resultaten dit met zich mee bracht.

In deze resultaten vonden we een file naam kiwi\_passwords.yar.ink. omdat dit een .yar file is en het betrekking heeft tot paswoorden hadden we een vermoeden dat het deze file kon zijn. In de meta data van dit bestand hebben we ons resultaat niet gevonden.

In dit resultaat hebben we wel het path van mimikatz\_trunkx (desktop van H4S4N) gevonden en zijn

we dit ook eens gaan controleren.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Er stond geen mimikatz\_trunk op de dekstop. Dus hebben we dit ook eens gezocht via keyword. Hier hebben we bij results een 7z file van mimikatz\_trunk gevonden met locatie “Downloads”.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

In downloads hebben we een zip file gevonden van mimikatz\_trunk waarin opnieuw het bestand kiwi\_passwords.yar stond wat we eerder ook al zagen in het path van Desktop.

Toen we dit openden vonden we gegevens zoals description en author -> wat we nodig hebben.

1.15:

Probleem:

1. Wat is een MS-NRPC based exploit?

Oplossing:

1. We hebben dit gegoogelt en hebben een artikel gevonden over een bedrijf waarvan er een niet-geverifieerd compromise was van de domain controllers. Hier werd er een nadruk gelegd op de naam “Zerologon”.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

We hebben dit eens gezocht via keyword search en vonden een resultaat.

Afbeelding met tekst

Automatisch gegenereerde beschrijving