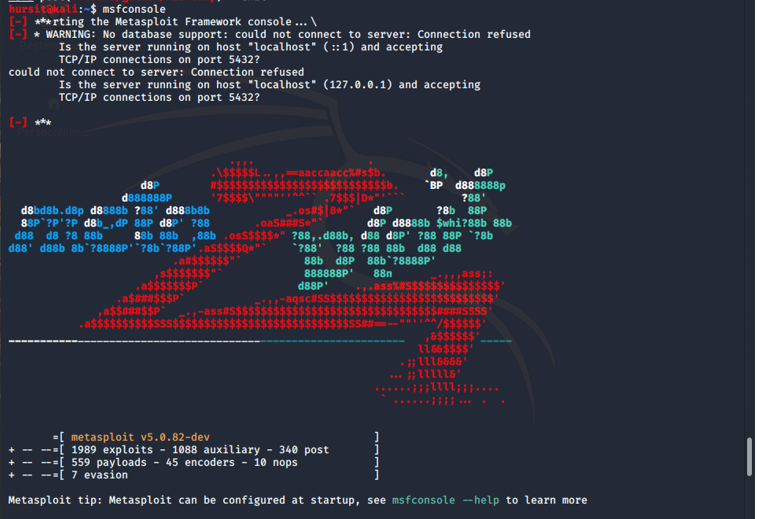
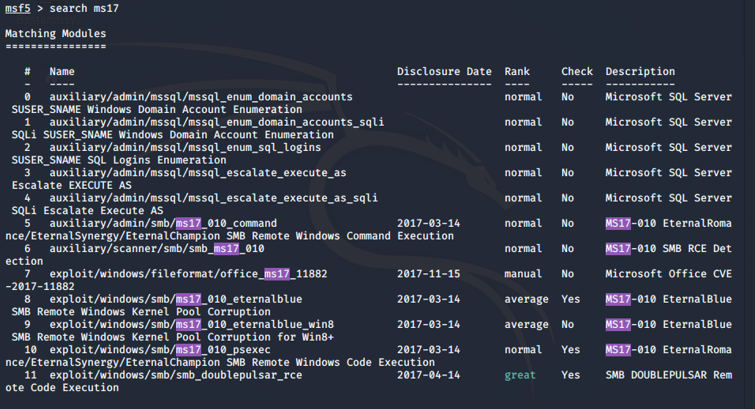
**Red Teaming Aspect: Ethical Hacking**

**Level C Requirements:**

Het eerste wat we nu moeten doen is verbinding maken met de target host. Om verbinding te kunnen maken met de target host moeten we eerst het IP-adres kennen. Dit IP-adres (192.168.100.6) staat gegeven bij de scans die we hebben gekregen van Team Blue. Nadat we het IP-adres hebben gaan we gebruik maken van de ‘Metasploitable Framework Console’ (msfconsole).



Ik heb in de scans gezien dat er remote code execution mogelijk is. Hiervoor heb ik op internet gezocht wat de beste modules hiervoor zijn en een veel gebruikte module is: MS17\_010\_Ethernalblue, deze maakt gebruik van SMB. Om deze exploit te kunnen gebruiken moeten we eerst het volledige pad vinden. Hiervoor typen we het commando ‘search ms17’, dit geeft een lijst met alle modules die met ‘ms17’ beginnen.



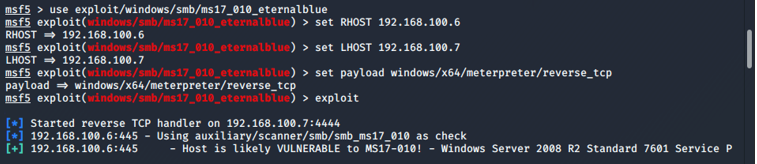
Op bovenstaande screenshot zien we het pad, namelijk ‘exploit/windows/smb/ms17\_010\_ethernalblue’. Dit gaan we nu gebruiken door ‘use + pad’ in te geven.

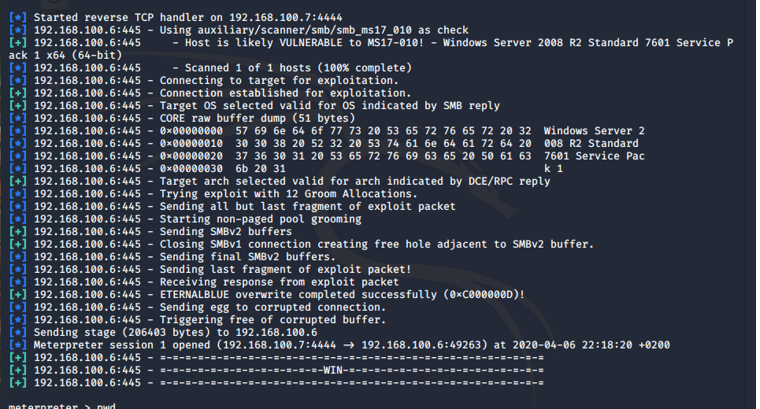


Als we nu ‘options’ intypen dan krijgen we de parameters die we moeten ingeven voordat we de exploit kunnen runnen. In dit geval zijn er drie parameters die we moeten ingeven:

* RHOST: Dit is het IP-adres van de target host, dus de pc die wordt aangevallen.
* LHOST: Dit is ons eigen IP-adres, dus 192.168.100.7.
* Payload: Simpel gezegd is dit een script dat voor interactie te voeren met het gehackte systeem, de payload die ik ga gebruiken is: ‘windows/x64/meterpreter/reverse\_tcp’.

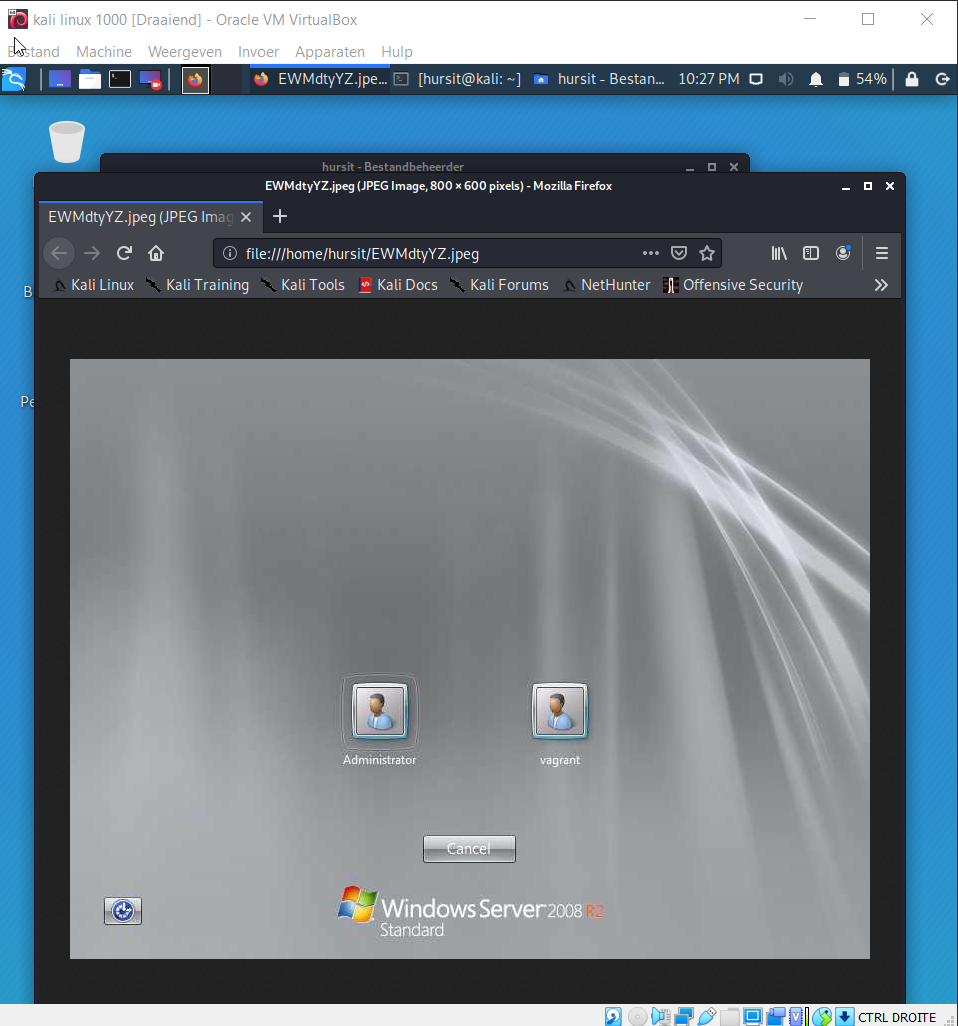
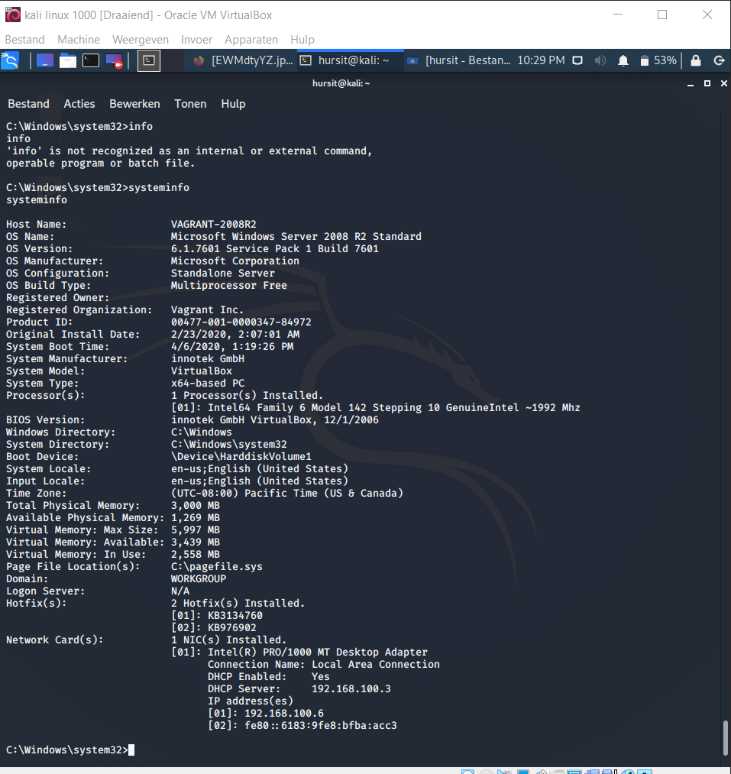
Nadat dit allemaal is ingevuld kunnen we ‘exploit’ typen om de exploit te starten.



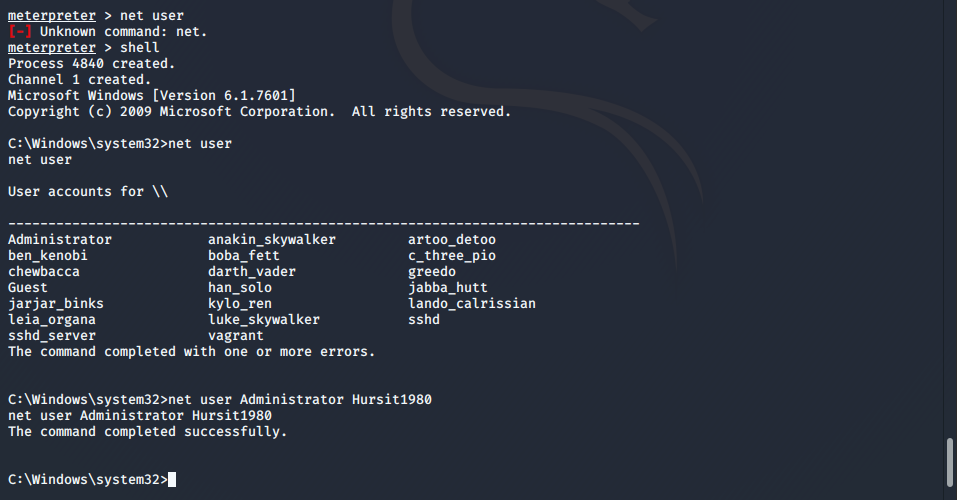


Als alles goed verlopen is krijgen we nu ‘meterpreter’ te zien voor ons haakje. Als we nu ‘pwd’ intypen dan zien we dat onze huidige dir, ‘C:\Windows\system32’ is. Dit wil zeggen dat we zijn binnengeraakt in een Windows OS. Om zeker te zijn dat het om de juiste PC ging heb ik een screenshot genomen om dit te bevestigen.

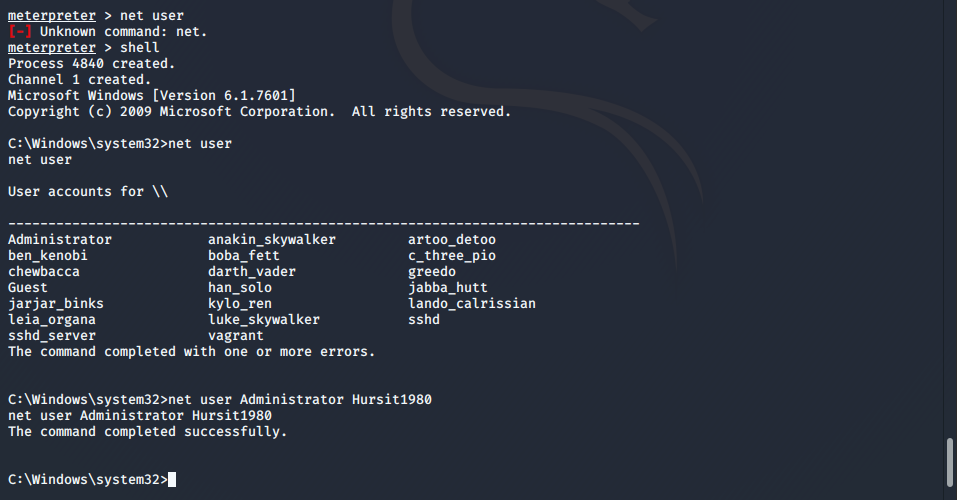




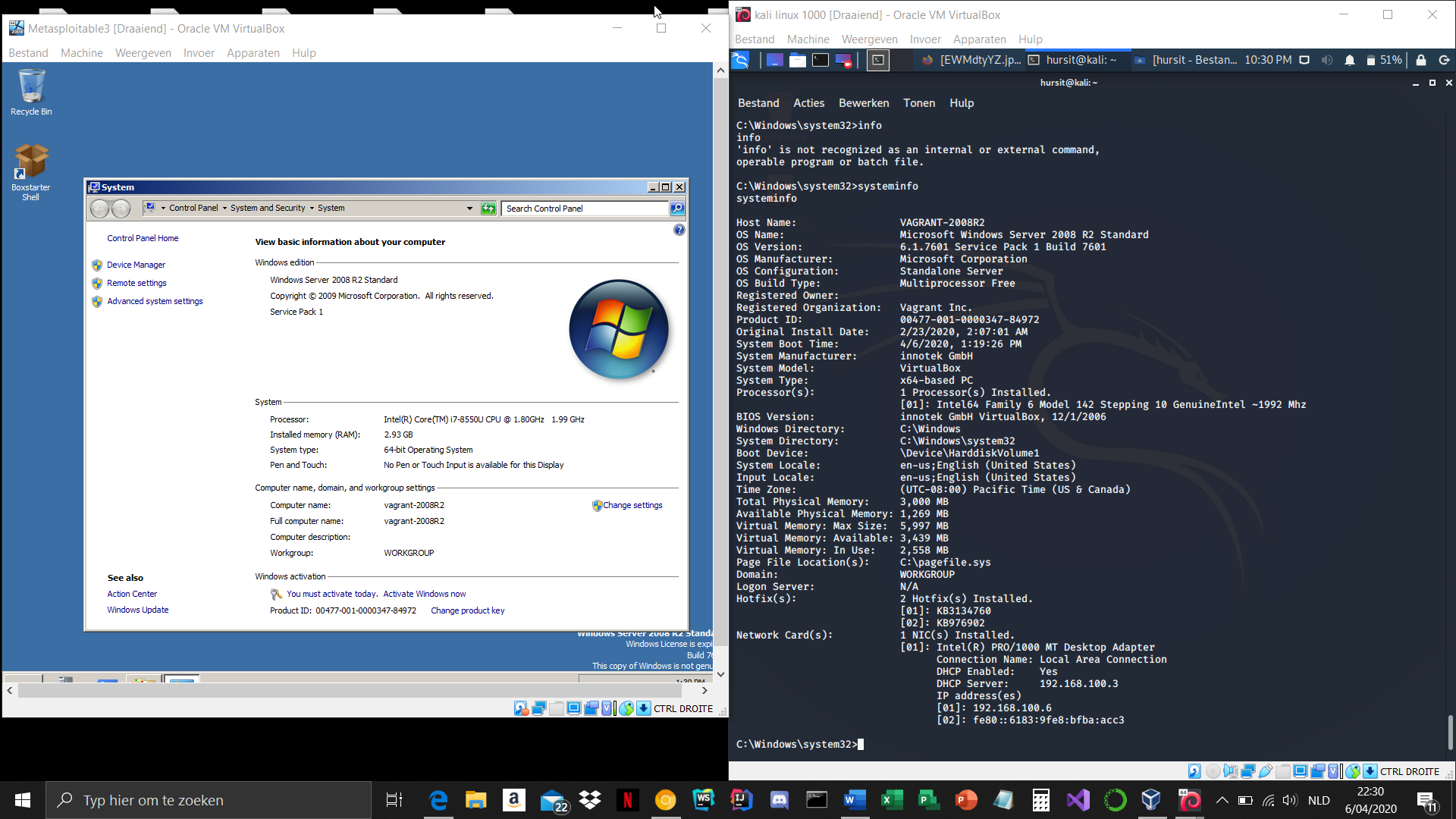
Stap 1 is nu voltooid, we zitten in het juiste systeem. Stap twee is het verkrijgen van Administrator rechten. Hiervoor typen we eerst het commando ‘net user’, dit commando geeft ons een overzicht van alle gebruikers.



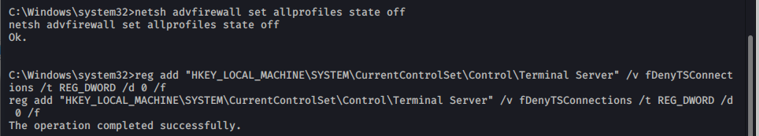
Om nu het wachtwoord van de Administrator te kunnen veranderen voeren we het volgende commando in: ‘net user Administrator’ + ‘wachtwoord naar wens’. Ik heb hier mijn naam met hoofdletter + een random jaartal gebruikt.



Als alles goed gegaan is, dan hebben we nu toegang tot het administrator account met het wachtwoord dat we juist zelf hebben gekozen.

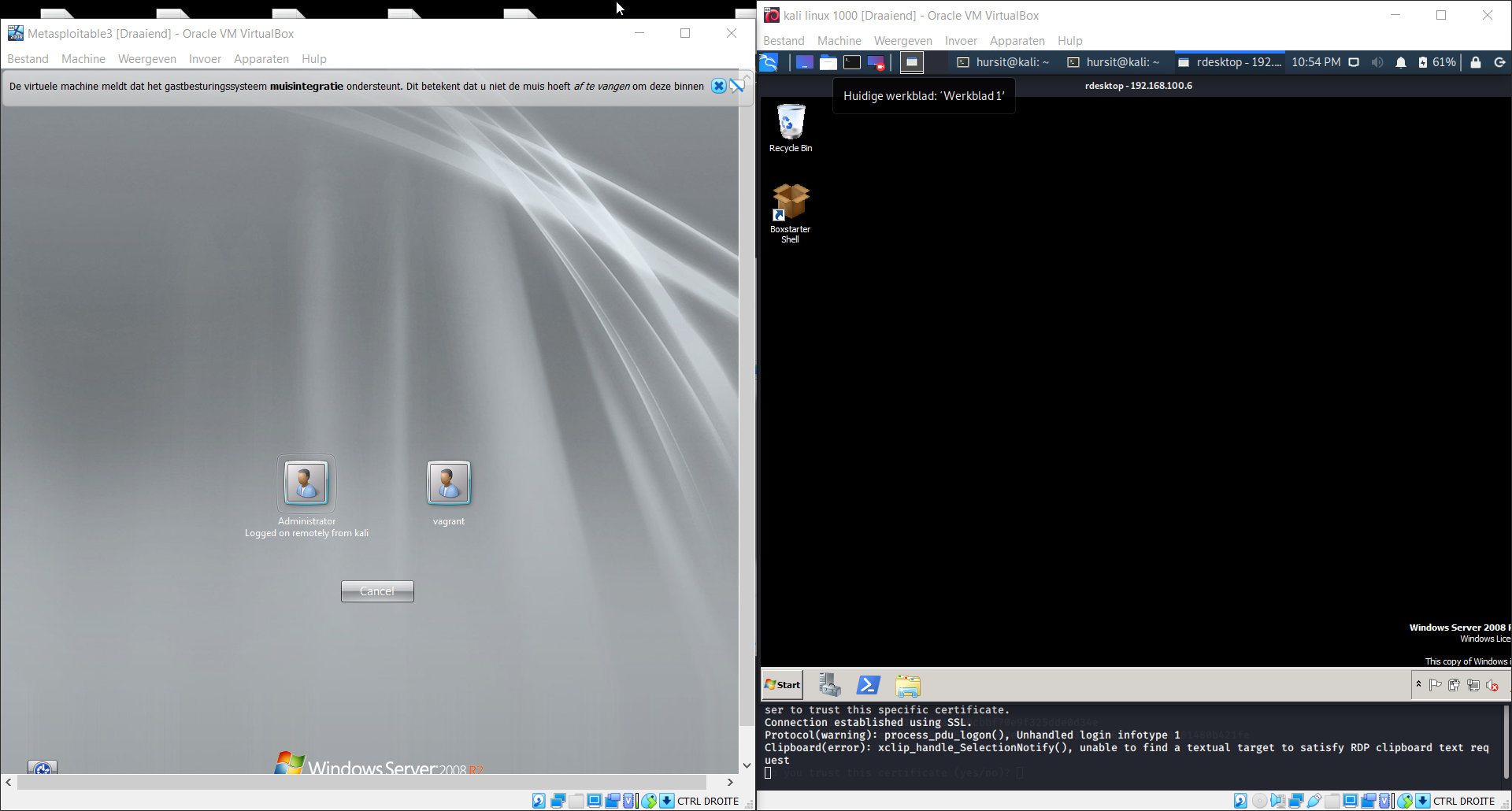


Stap 2 is nu ook voltooid. Stap 3 is om een Remote Desktop sessie op te starten. Vanaf het moment dat we in het systeem zitten is dit eigenlijk heel gemakkelijk. Het enige wat we hiervoor moeten doen is het volgende commando invoeren in onze terminal.

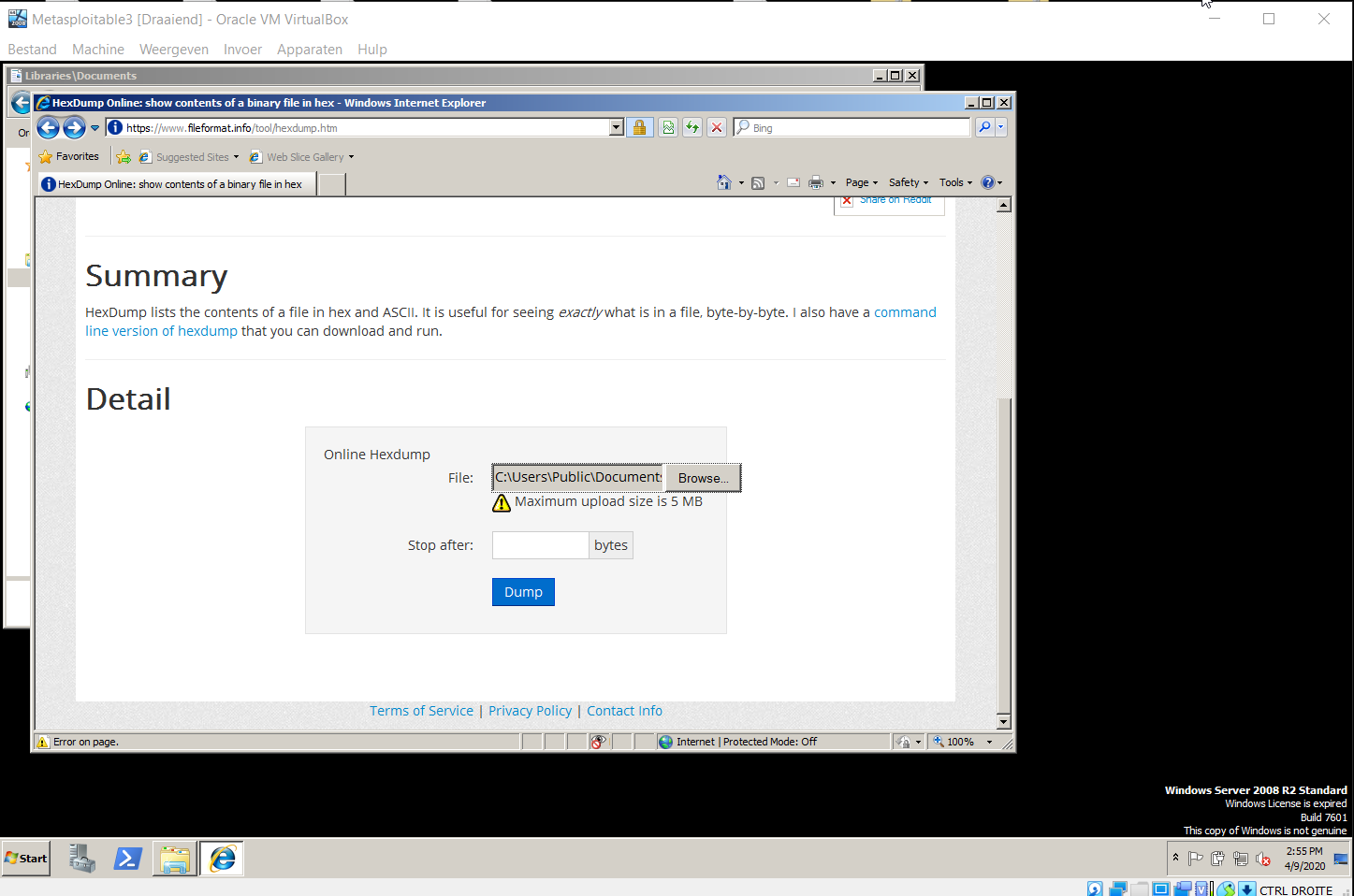


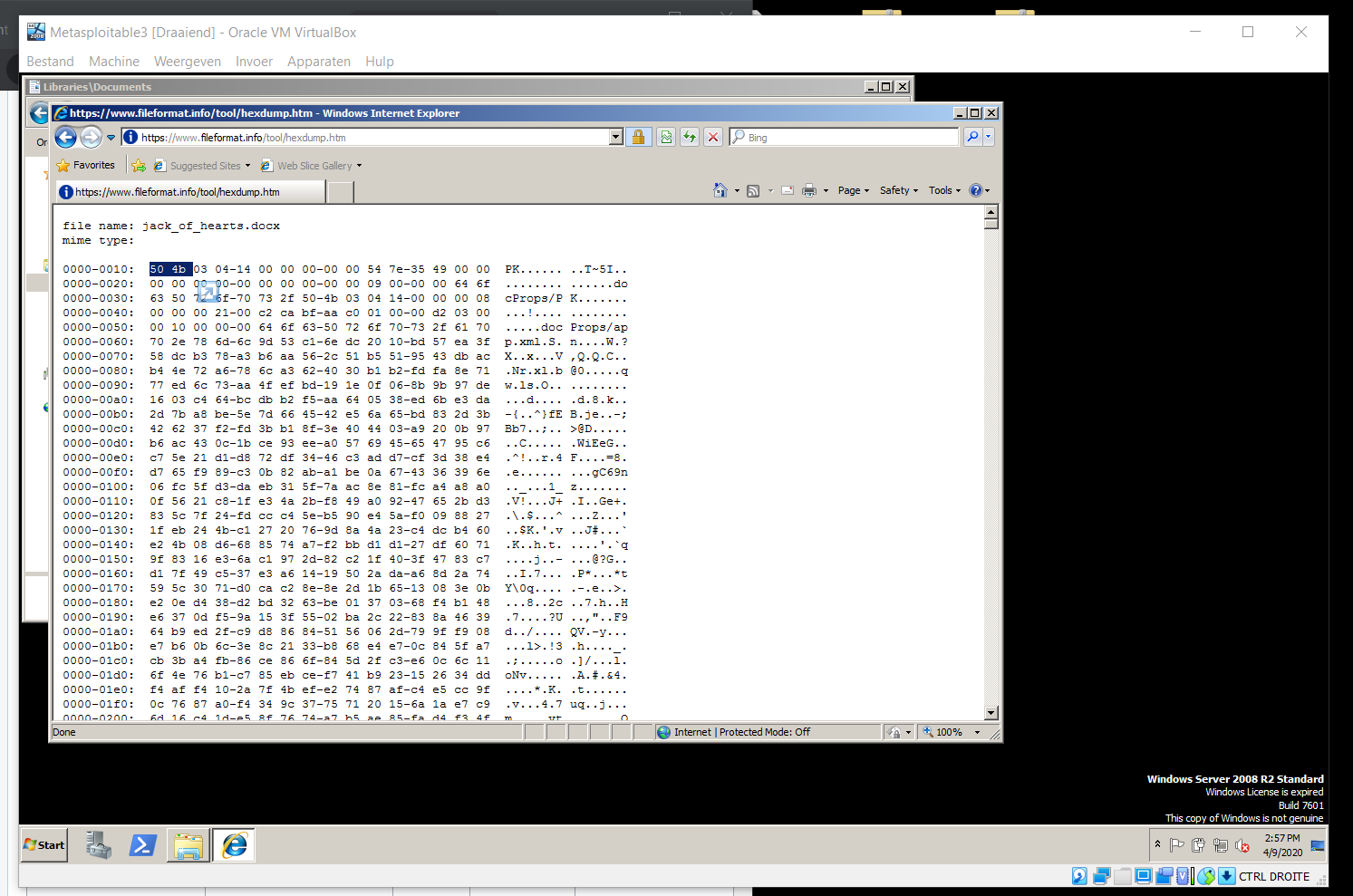
Als we nu ‘exit’ typen en onze meterpreter verlaten en we typen het commando ‘rdesktop + IP van target’ en daarna ‘yes’ dan krijgen we het scherm van het target OS te zien en we kunnen bv. aan elk bestand, etc…

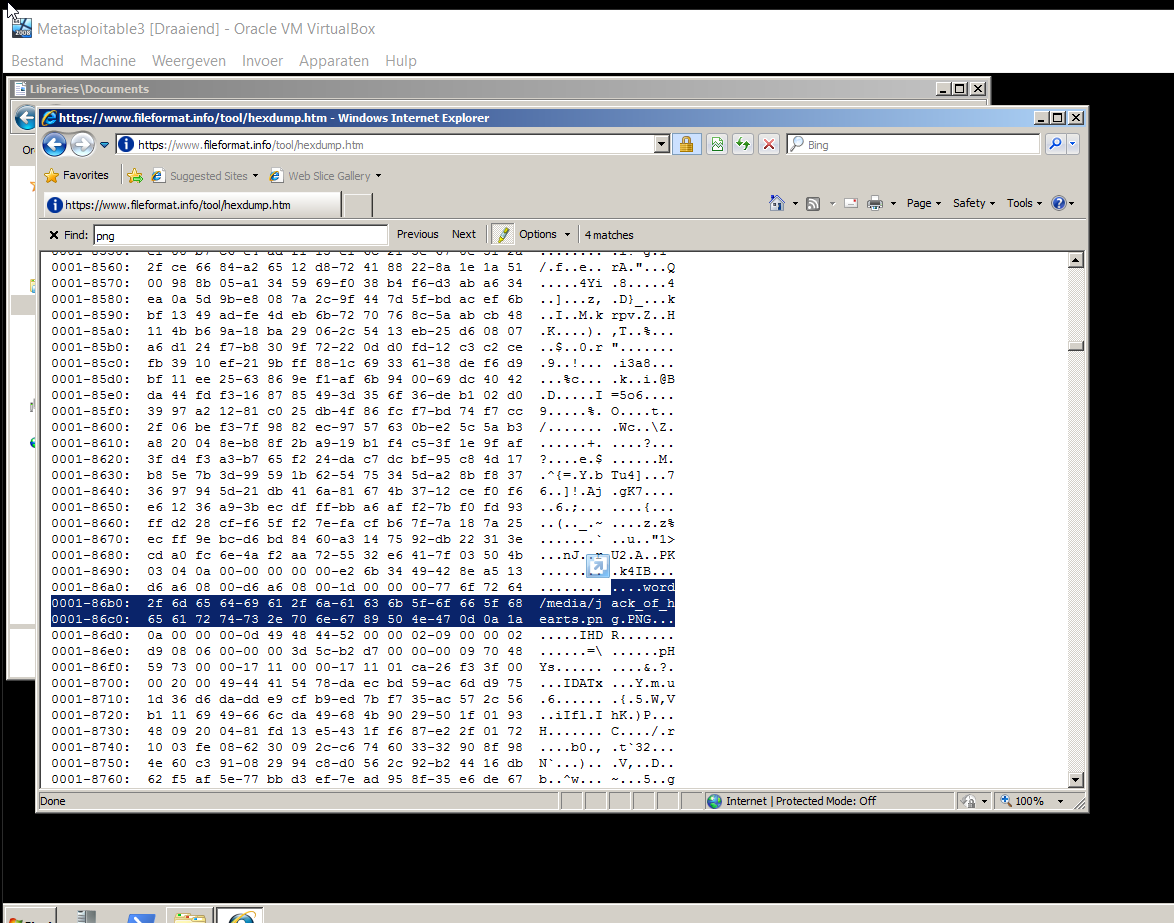




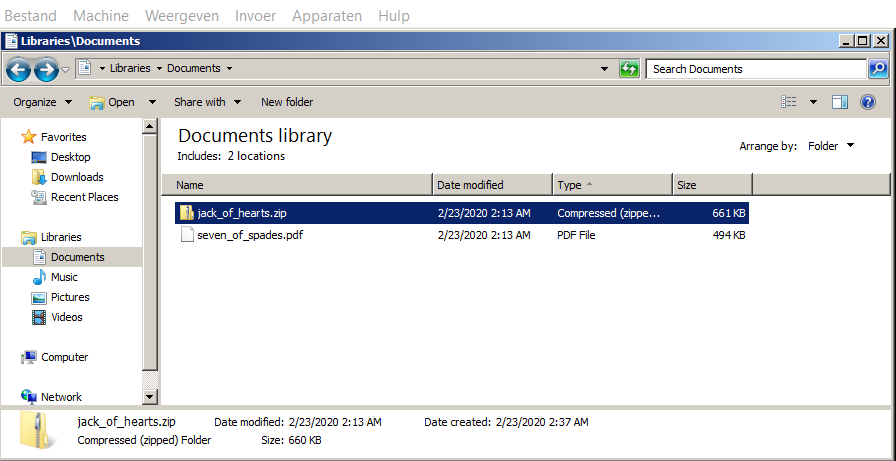
Stap 3 is nu ook gedaan. Voor stap 4 moeten we minstens 1 van de 15 hidden flags vinden. We weten door de opgave dat het gaat om afbeeldingen van speelkaarten. Als we naar ‘Documents’ gaan, dan zien we al twee namen van speelkaarten. Namelijk ‘Jack of hearts’ en ‘Seven of spades’. We kunnen op ‘Jack of hearts’ klikken, dit geeft een afbeelding maar niet van een speelkaart. Ik heb deze file in een hexdump gezet om alles even te bekijken.



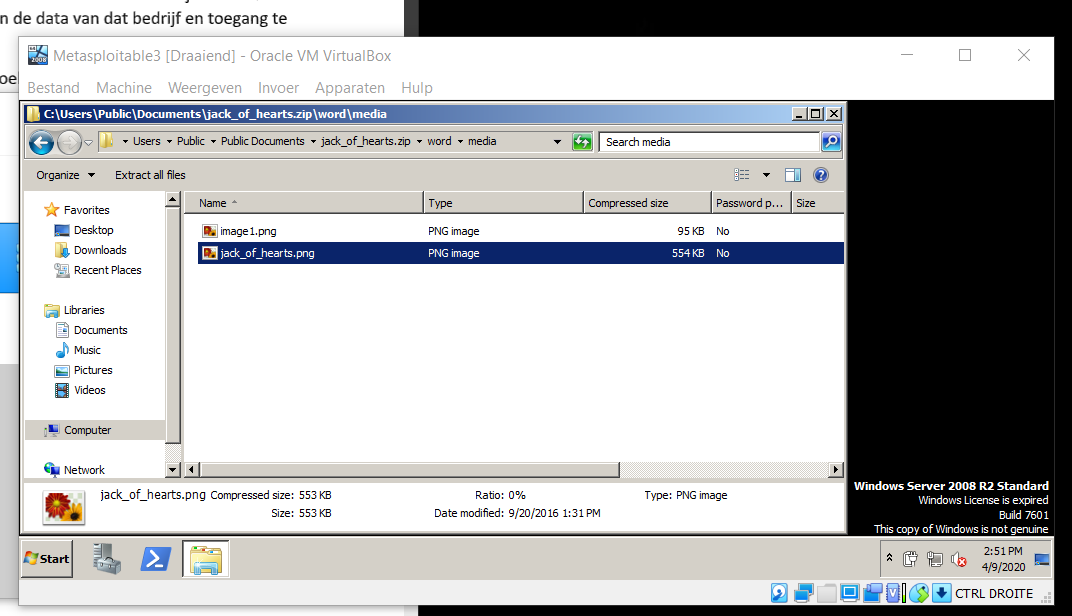




Als we hier naar het eerste deel kijken wat aangeduid staat dan zien we ’50 4b 03 04’. Na dit op te zoeken op Google kreeg ik te zien dat het ging om een Zip. In de tweede afbeelding zien we ook dat er staat ‘jack\_of\_hearts.png’. Dus het eerste wat in mij opkwam was om de extensie te wijzigen naar een .zip.



Ik zag inderdaad dat er verschillende mappen zaten in deze zip en ook twee .png files.



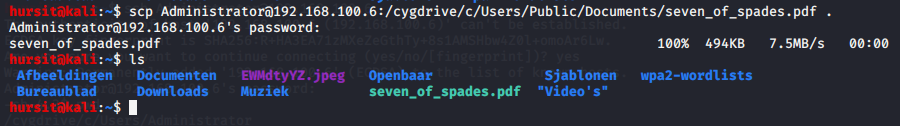
Dit is het resultaat als we de file openklikken:



De volgende die ik heb gevonden is seven\_of\_spades.pdf. Om deze te kunnen openen ga ik msfconsole gebruiken. We gaan via ssh inloggen met onze target host.

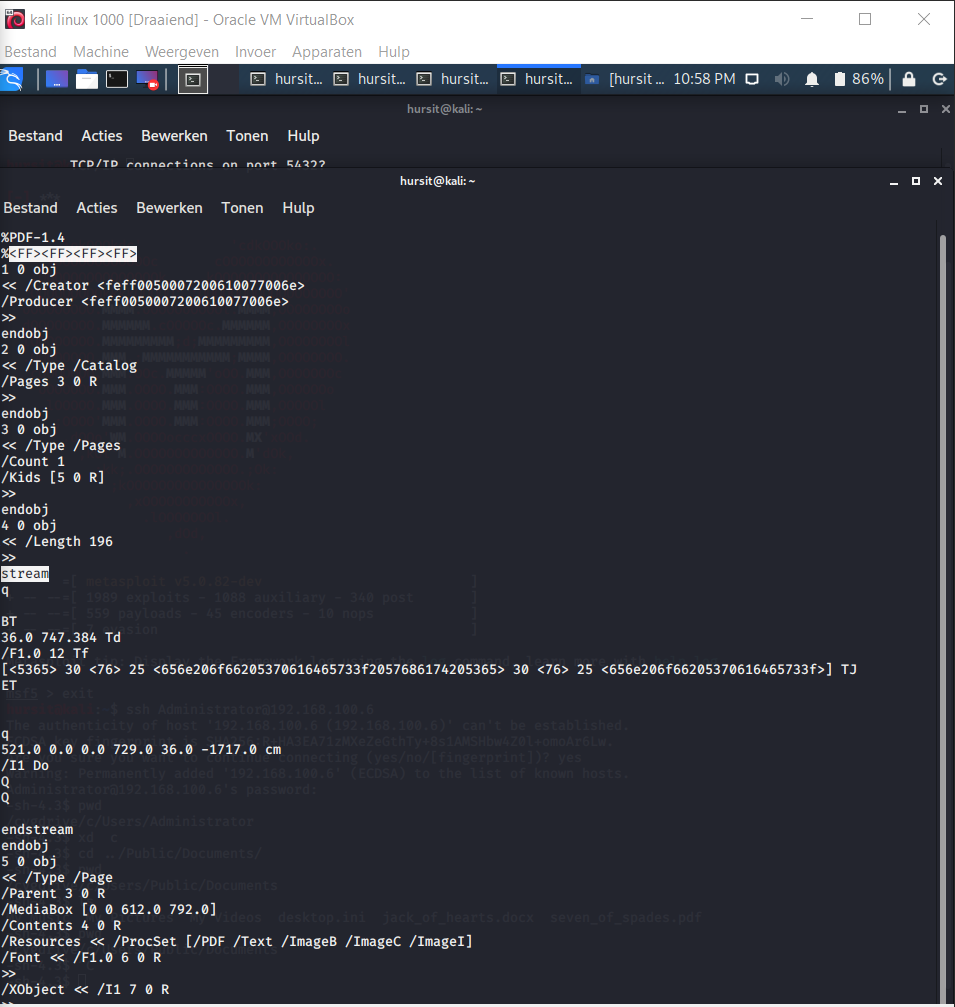


We gaan een kopie maken van de .pdf, hiervoor gaan we uit onze sessie.

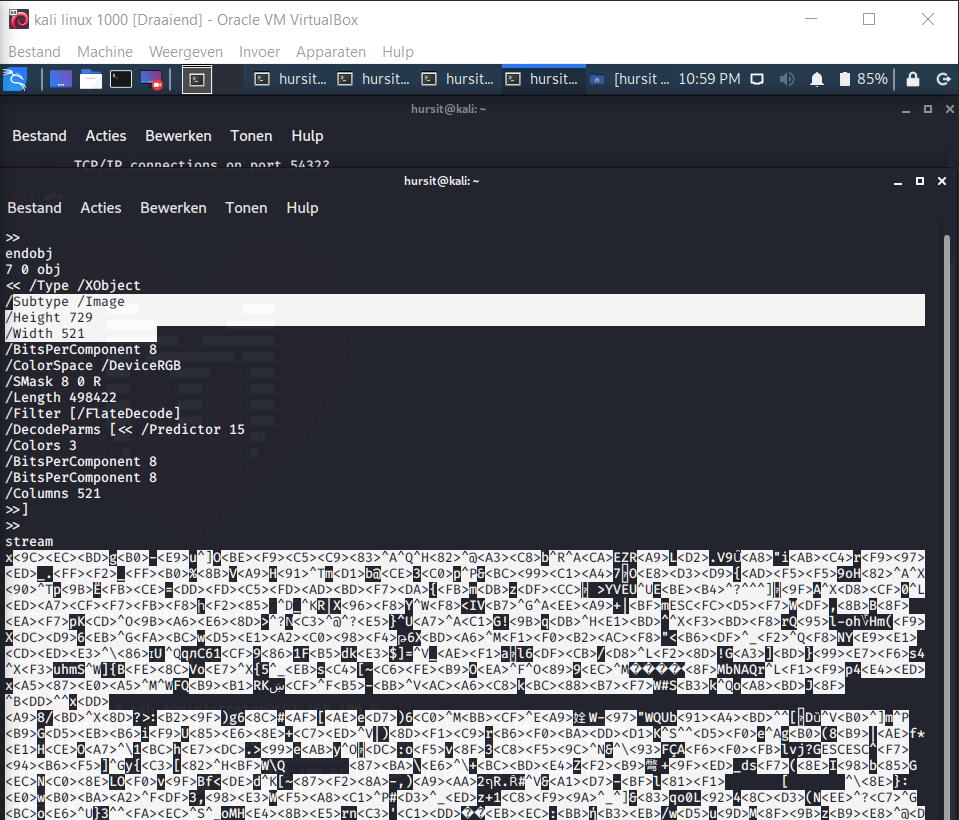


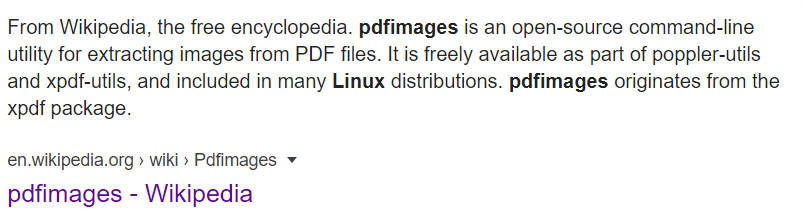


We openen ons bestand met het comando less en we bekijken de code.

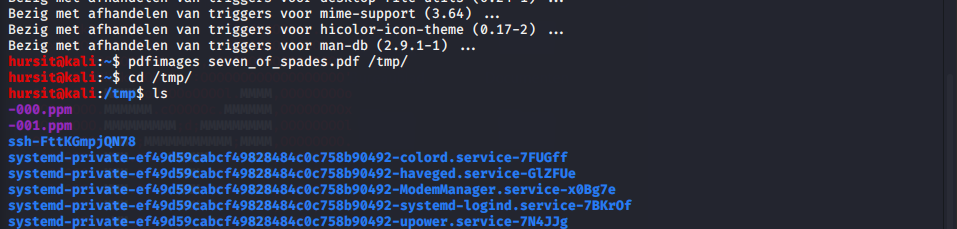


Hier kunnen we vanboven zien dat het om een .pdf file gaat door de header. We zien wel bij het tweede aangeduide deel dat er ‘stream’ staat. Een stream duid aan dat er iets anders zit verborgen in deze .pdf. We zien ook Image staan als we verder naar onder beginnen te scrollen, dus we zitten waarschijnlijk op het juiste pad.

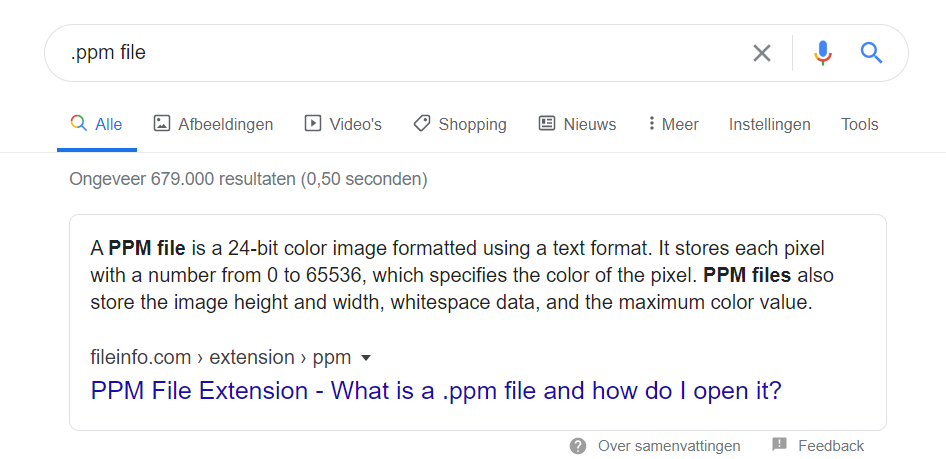




Nu gaan we gebruik maken van het commando ‘pdfimages’ om deze images uit onze .pdf file te halen.



Hier zien we dat wanneer we de dir bekijken dat er 2 .ppm files zijn. Ik weet niet wat dit betekent dus we gaan dit opzoeken. (zie definitie op onderstaande foto).



We weten dat het over een foto gaat maar als we op de file drukken dan opent er helemaal niks. In onze GUI zien we wel al een preview van de afbeelding. Op internet stond dat er heel wat programma’s waren om .ppm files te openen maar ik heb gewoon de extensie veranderd naar .png en dit zorgde ervoor dat ik de afbeelding in fullscreen kon bekijken.

