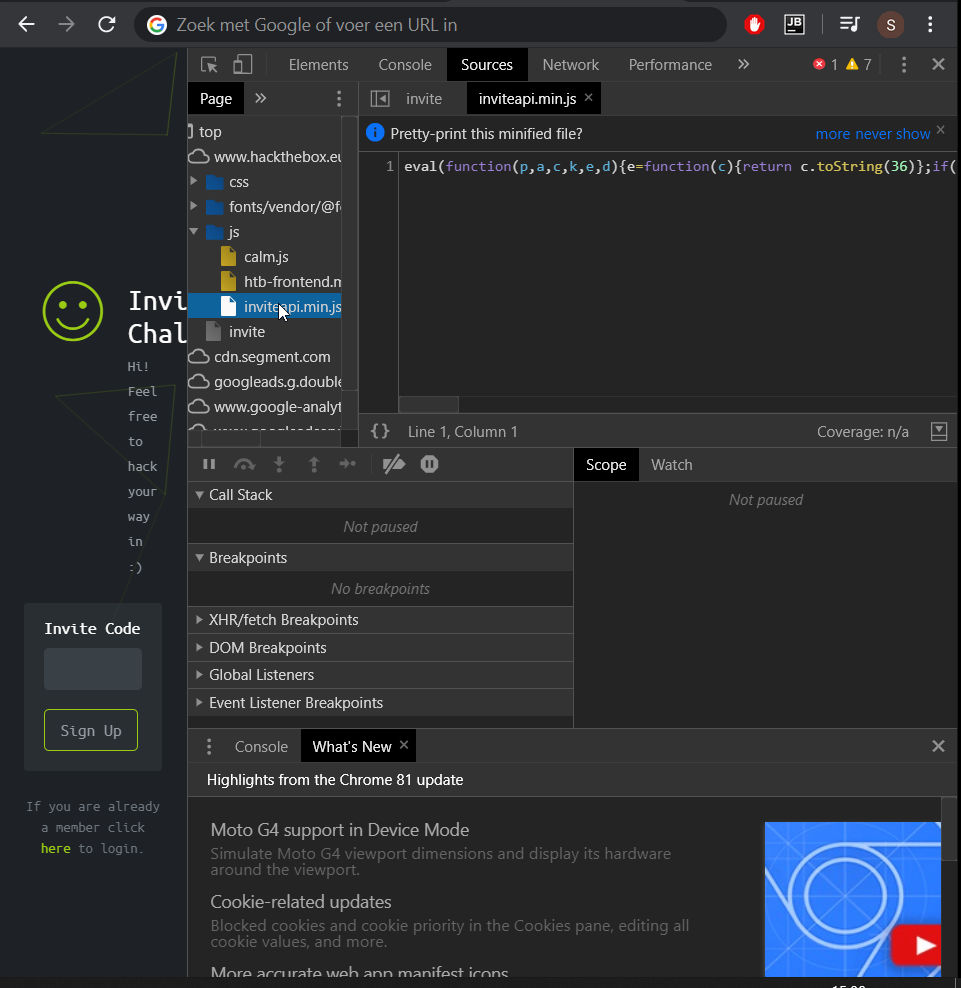
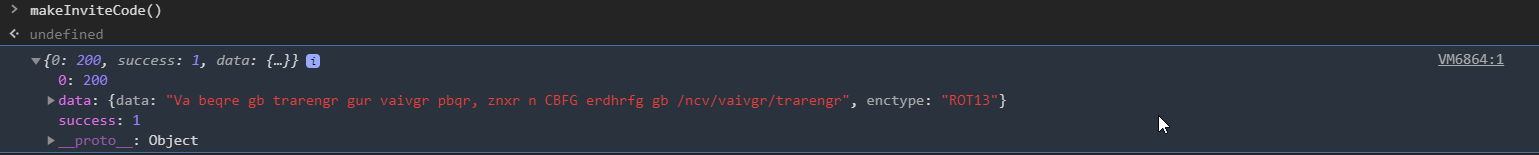
**Red Teaming Aspect: Ethical Hacking**

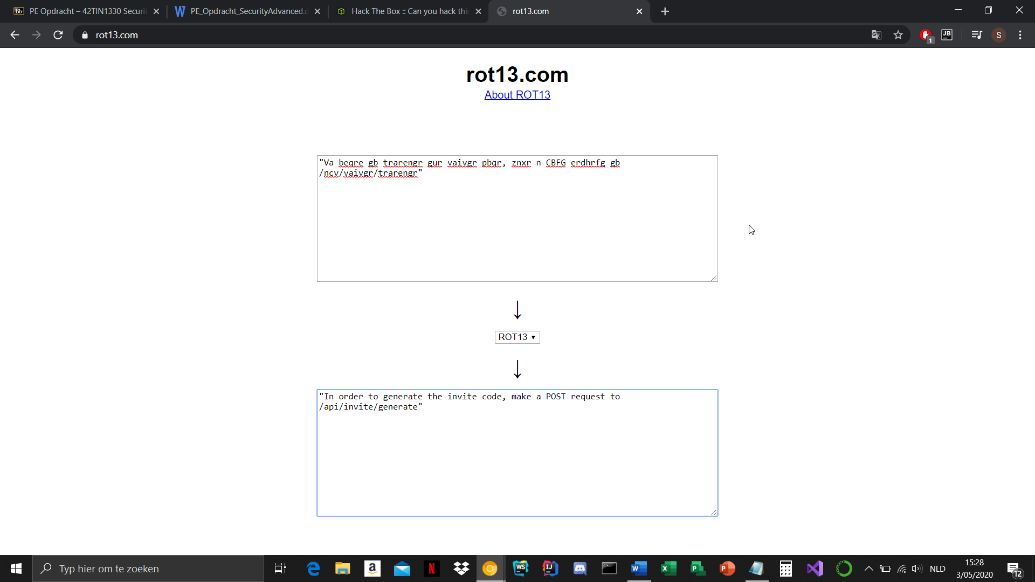
**Level B Requirements:**

De eerste stap is om een Hack The Box account te maken. Dit hebben we vorig jaar in de lessen security ook gezien, daarom ga ik het kort even herhalen.

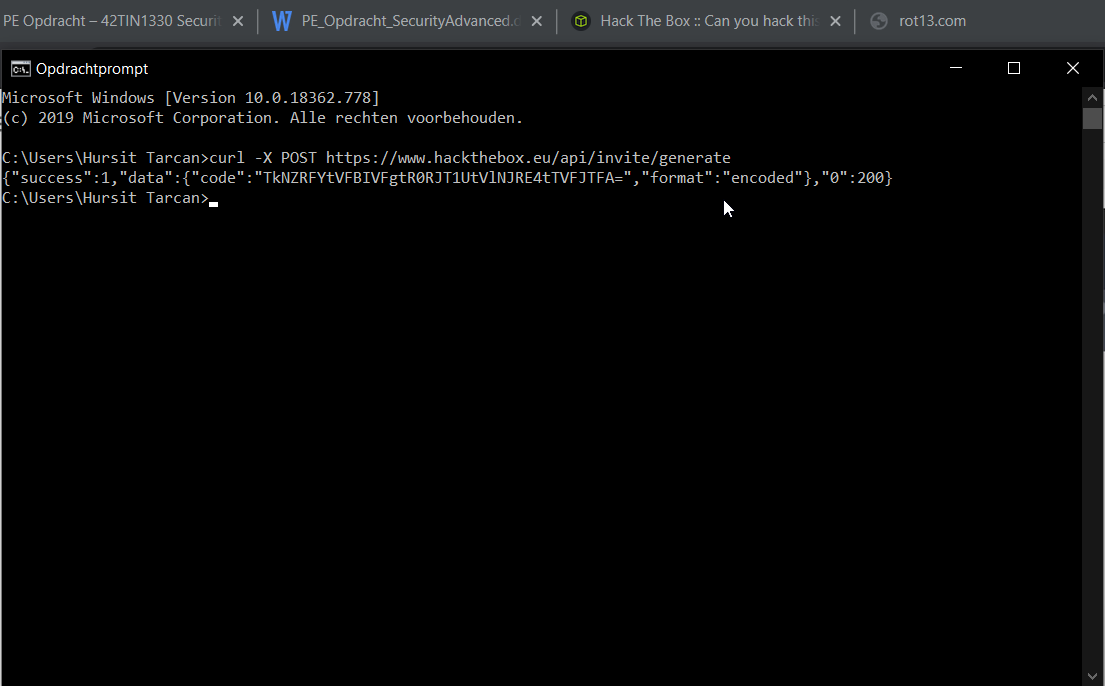


Wanneer we ‘Element Inspecteren’ klikken op de login pagina dan zien we dat er een script is dat ‘inviteapi.min.js’ noemt. Als we dit nu bekijken dan zien we dat er een functie inzit die makeInviteCode() noemt. Wanneer we deze functie oproepen dan krijgen we volgend resultaat terug:

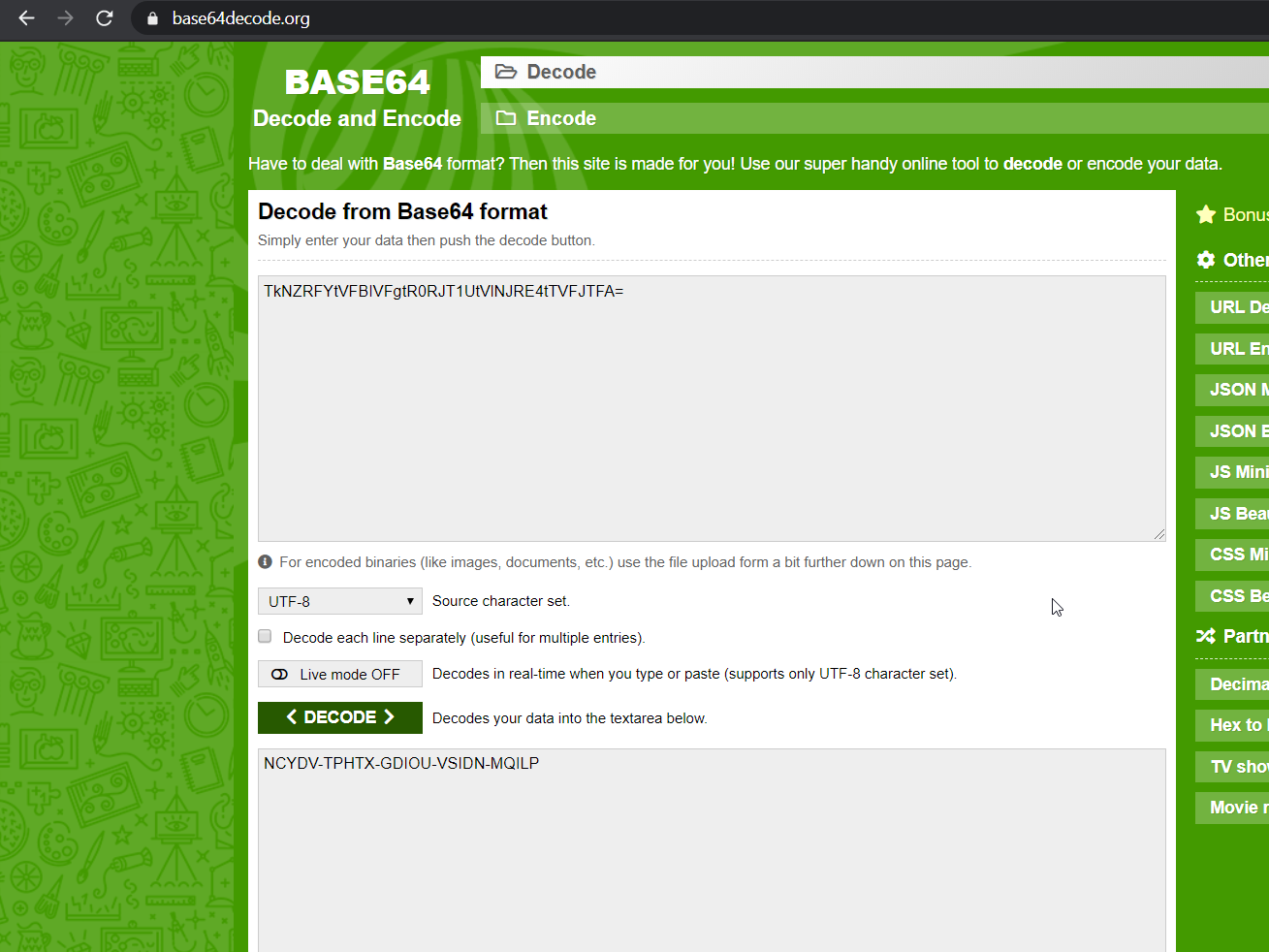


We krijgen een string en een encryptie type.

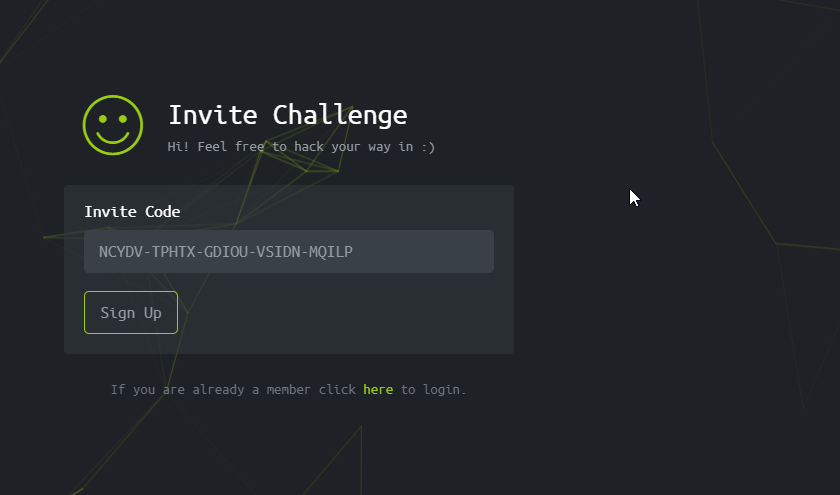
Hierin staat dat we een post request moeten doen om onze invite code te ontvangen.

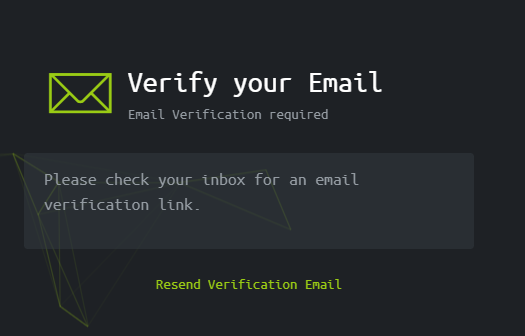


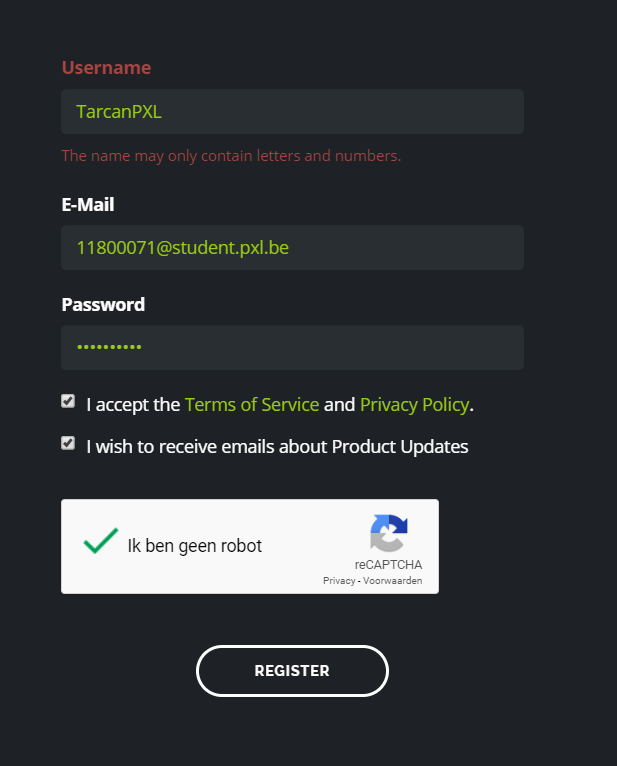
We hebben nu weer een response gekregen met ook de info dat het weer geencrypteerd is. We gaan dit weer decrypteren.

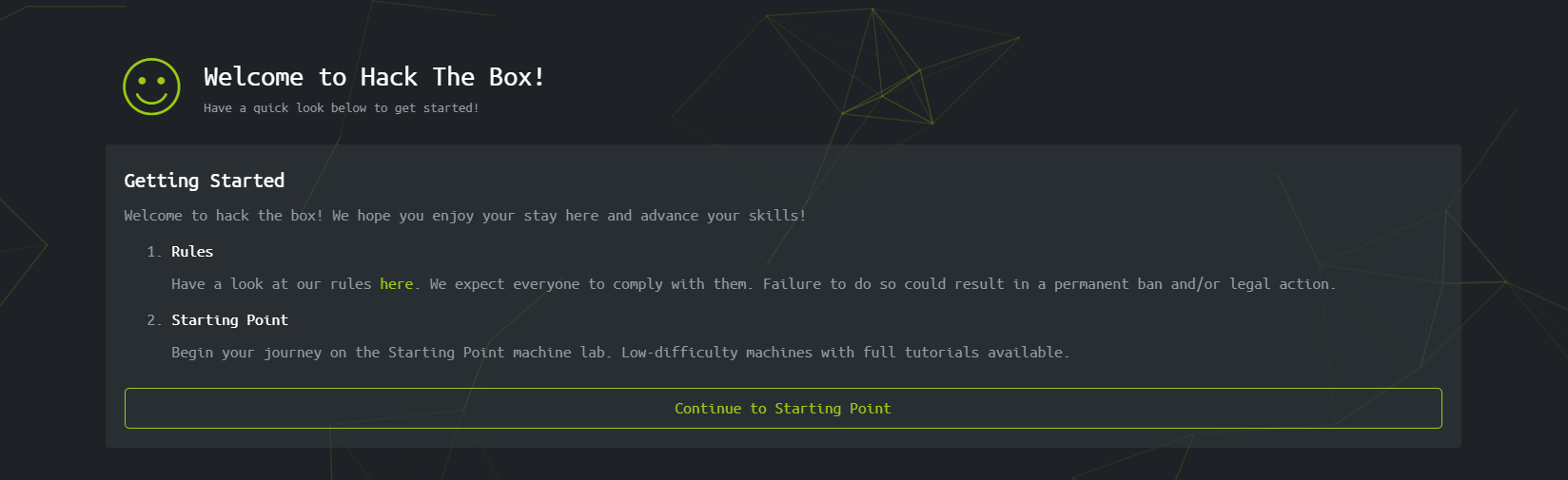


Als we deze key nu in onze input plakken op de login pagina dan kunnen we een account aanmaken.







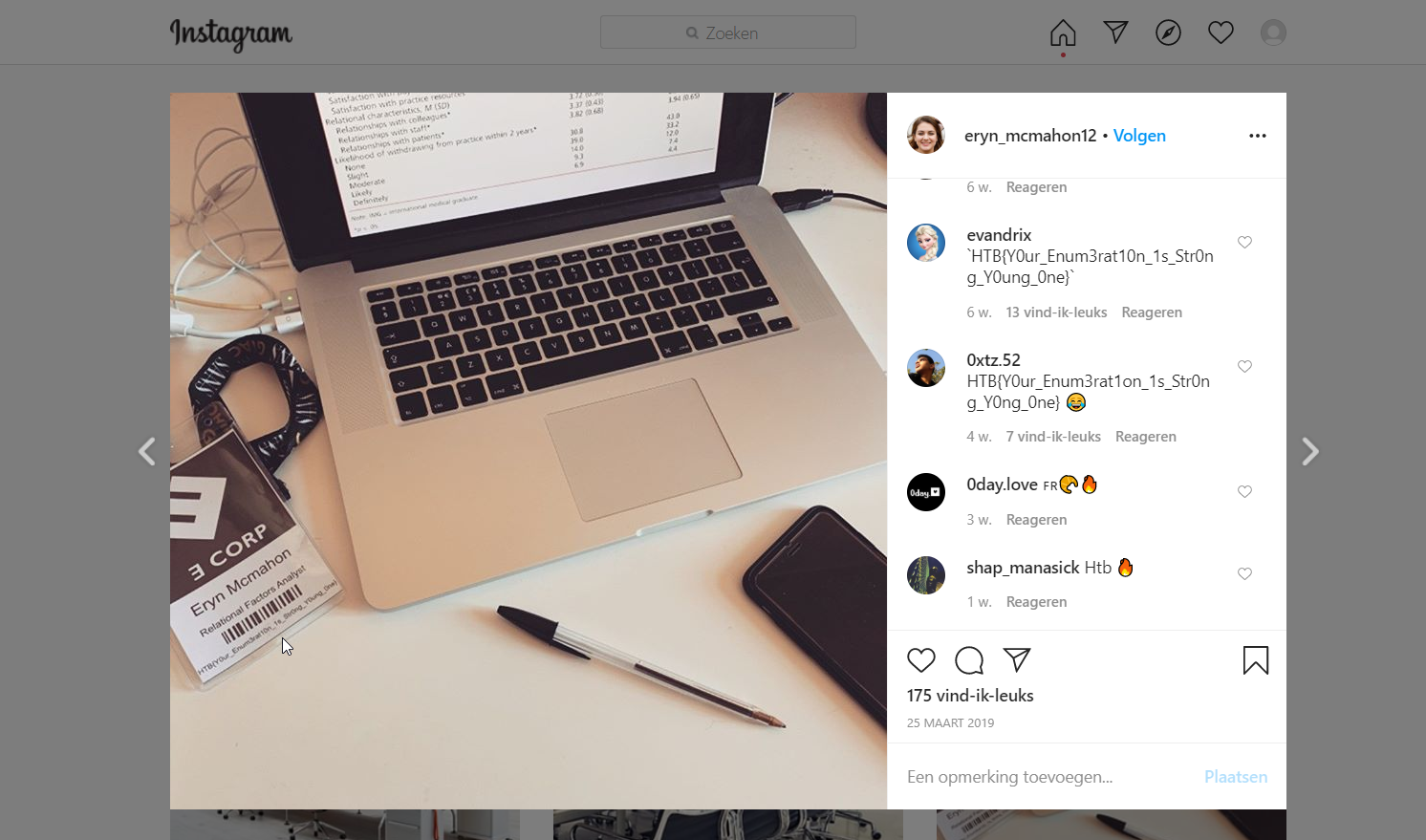


Nu we ons account hebben aangemaakt kunnen we met het echte werk beginnen. De ‘OSINT challenges’ zijn het eerste deel van de B requirements. De eerste challenge die we gaan doen is Infiltration, deze challange was voor mij de makkelijkste.

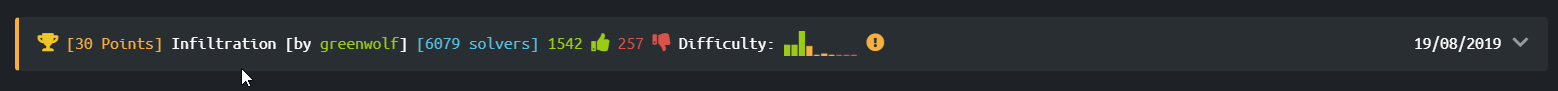
Wanneer we op google opzoek gaan naar ‘Evil Corp LLC’ dan zien we een Twitter account.

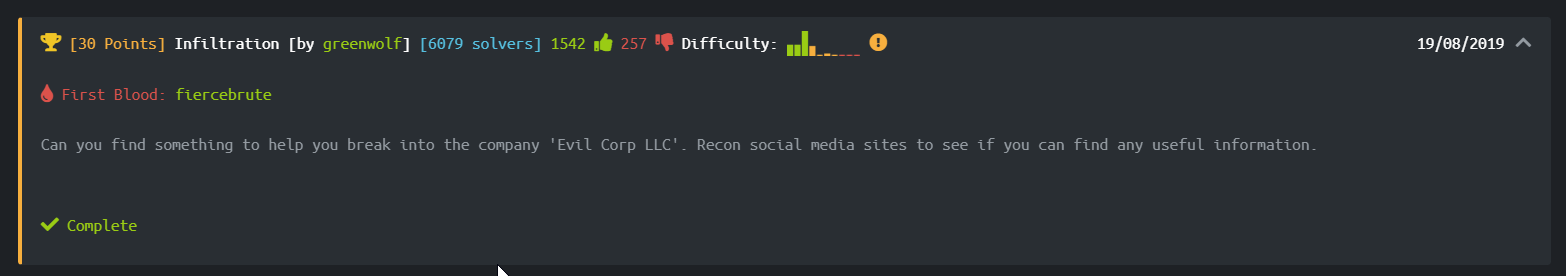


Het eerste wat we zien is een HTB flag. Deze flag is echter fout, en als we deze flag decrypteren krijgen we een bericht dat we moeten blijven doorgaan. Na wat verder zoeken komen we bij een Instagram account van een werknemer. Als we hier de foto’s gaan bekijken komen we bij een foto waarop de flag te zien is. (Zie cursor)



Als we deze flag nu noteren in het inputfield dan krijgen we te zien dat we de challange hebben gehaald.





De eertse challange is nu gedaan. Voor de tweede challange hebben we een zip die beveiligd is met een passwoord. Het eerste passwoord hebben we gekregen ‘hackthebox’.



Het tweede passwoord hebben we nodig voor username.zip. Dit heeft wat langer geduurd omdat het moeilijk te zien was wat de scope was waar we moesten zoeken. Na een tijdje zoeken kwam ik bij het profiel van een werknemer. Deze had een tweet waar ik direct al links onder ‘Ssh default pw’ zag. Dit passwoord was echter fout, maar als we de pijl volgen die deze richting uit kwam dan zien we ‘New Hire’ staan. 

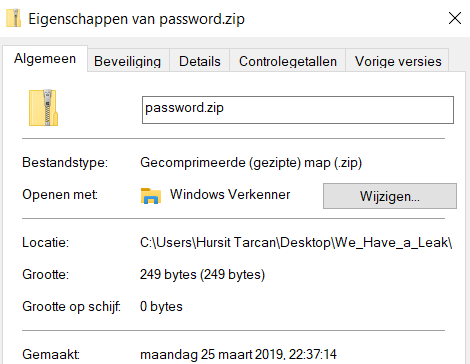
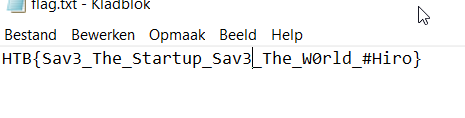
Wanneer we op de hoofdpagina zitten dan zien we een tweet van 26 maart over een nieuw lid.

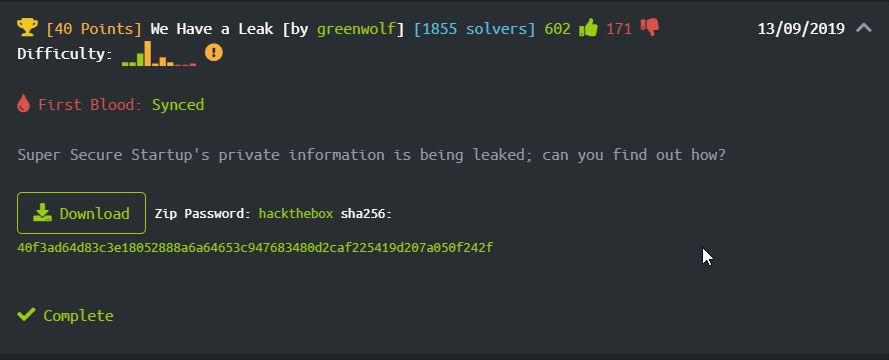


Dit nieuw lid is JTerranwald, wanneer ik dit profiel bekijk zie ik echter niks speciaals. En als we deze naam gebruiken als passwoord dan krijgen we nogsteeds niks te zien. Na wat verder zoeken zag ik volgende comments onder een tweet.



Alia Mccarty is iemand die haar CV wilt doorsturen en Johanna Boyce is een werknemer. Als we haar mail bekijken dan zien we dat het bestaat uit de eerste letter van haar voornaam + . + achternaam. Dit hebben we ook geprobeert voor JTerranwald. Als we ‘j.terranwald’ gebruiken als passwoord dan zien we dat dit juist is. Het volgende passwoord dat we nu nodig hebben hebben we al gedeeltelijk gezien. Als we terug naar het begin gaan, en de pijl verder volgen naar ‘ssh default pw’. Dan zien we ‘SupSecStart#Winter2018!’. Dit passwoord is weer fout, wanneer we het laatste deel veranderen dan krijgen we het wachtwoord. We moeten kijken naar wanneer dit bestand gemaakt is, we zien dat dit in de lente is gedaan in 2019. Wanneer we het passwoord ‘SupSecStart#Spring2019!’ gebruiken dan zijn we binnen. We hebben nu een .txt file waar de flag in staat.





De laatste OSINT challange die we moeten doen is ‘Breach’. We werken weer met een zip file. Als we deze unzippen zien we drie bestanden. Een tekstbestand met allemaal id’s, namen, enzovoort. Een ander tekstbestand dat beveiligd is en een mail.

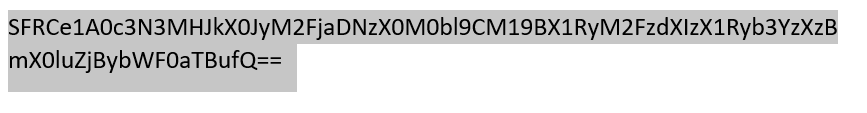
Omdat dit deel verder gaat op het bedrijf Super Secure Startup van de vorige challange, heb ik in het .txt bestand gezocht naar namen die bekend leken.



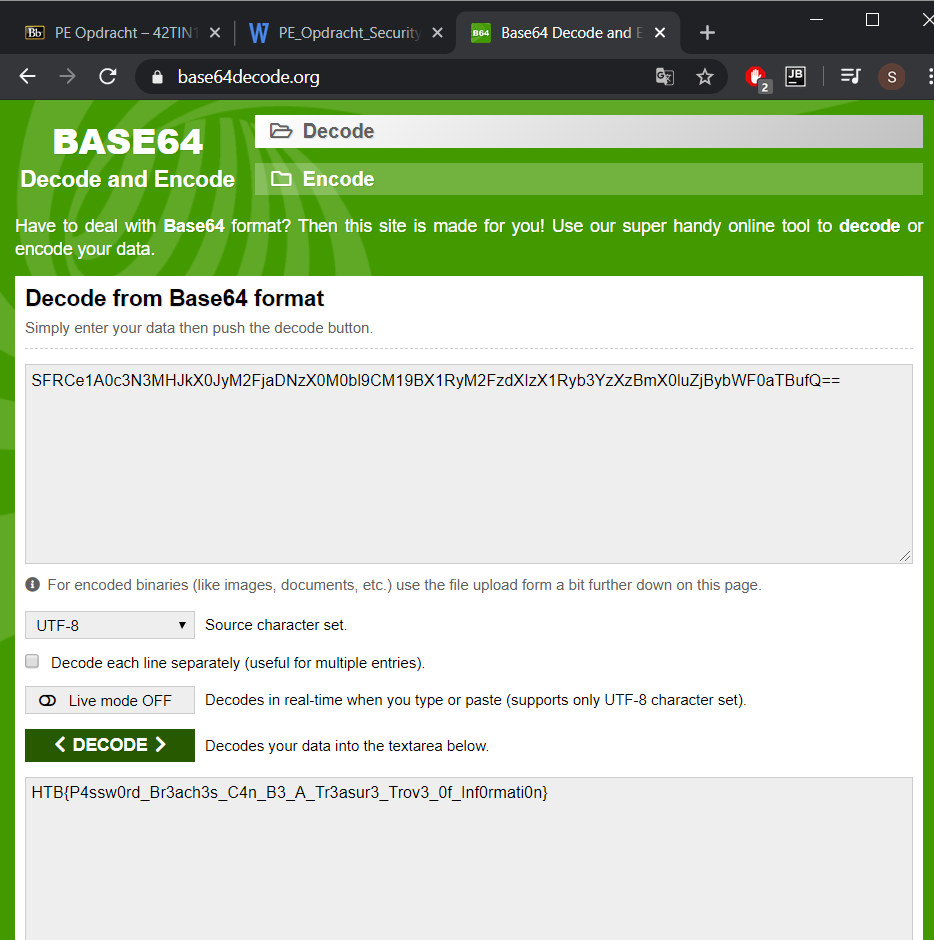
We vinden ‘Bianka Phelps’, en het wachtwoord ‘Love!July2018’. Dit passwoord heb ik getest maar negatief resultaat.



Omdat ik in dit wachtwoord een maand en jaartal zie deed het mij heel fel denken aan de vorige oefening waarbij het wachtwoord aangepast werd met de datum van de file. De datum dat de file aangepast werd is ‘Maart 2019’. Dus ik heb het wachtwoord aangepast en opnieuw geprobeerd, dit keer met wachtwoord: ‘Love!March2019’. Het wachtwoord was zoals ik had gedacht juist.

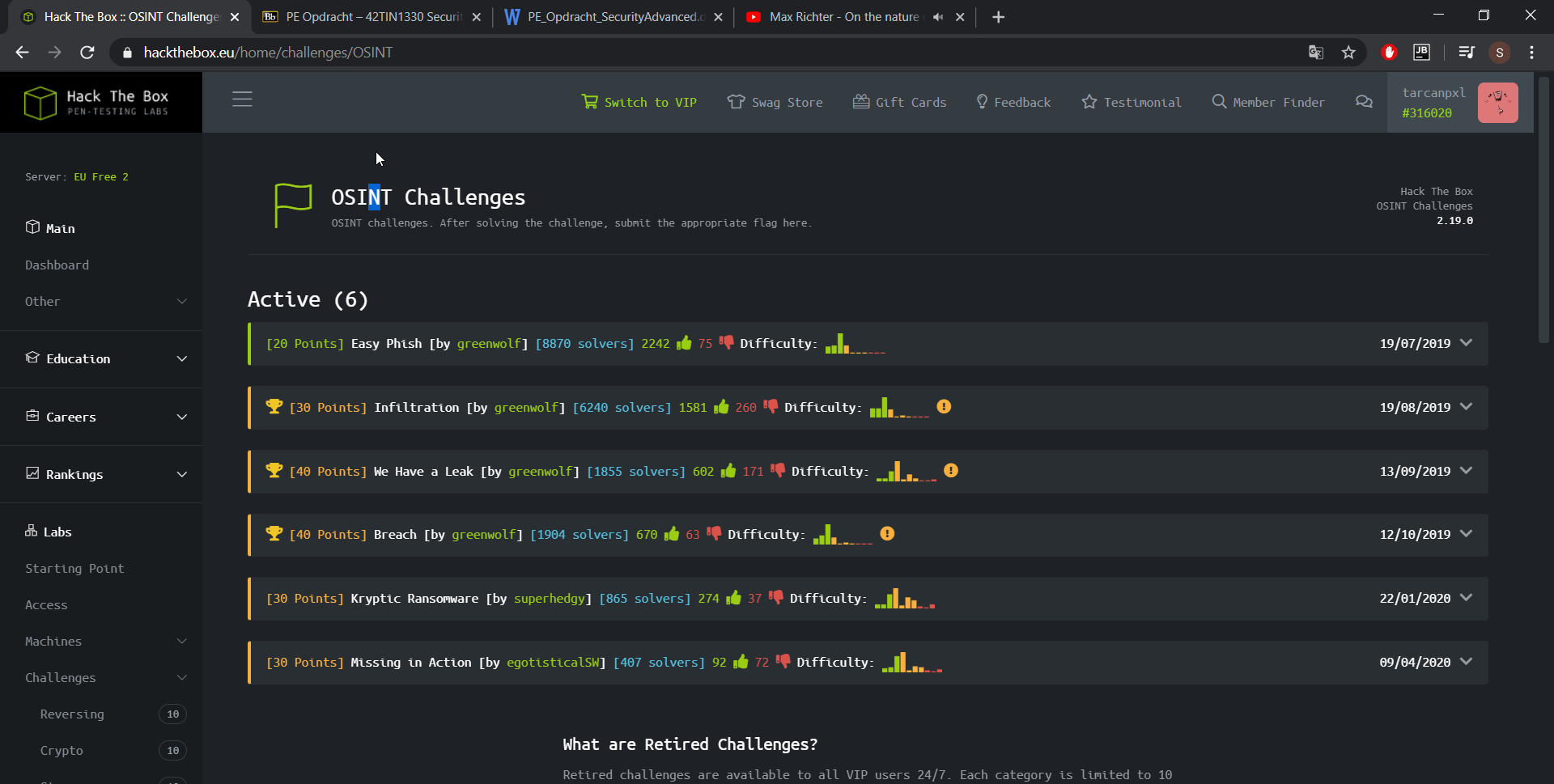


Dit was de tekst in het document. Nu gaan we dit moeten decrypteren.



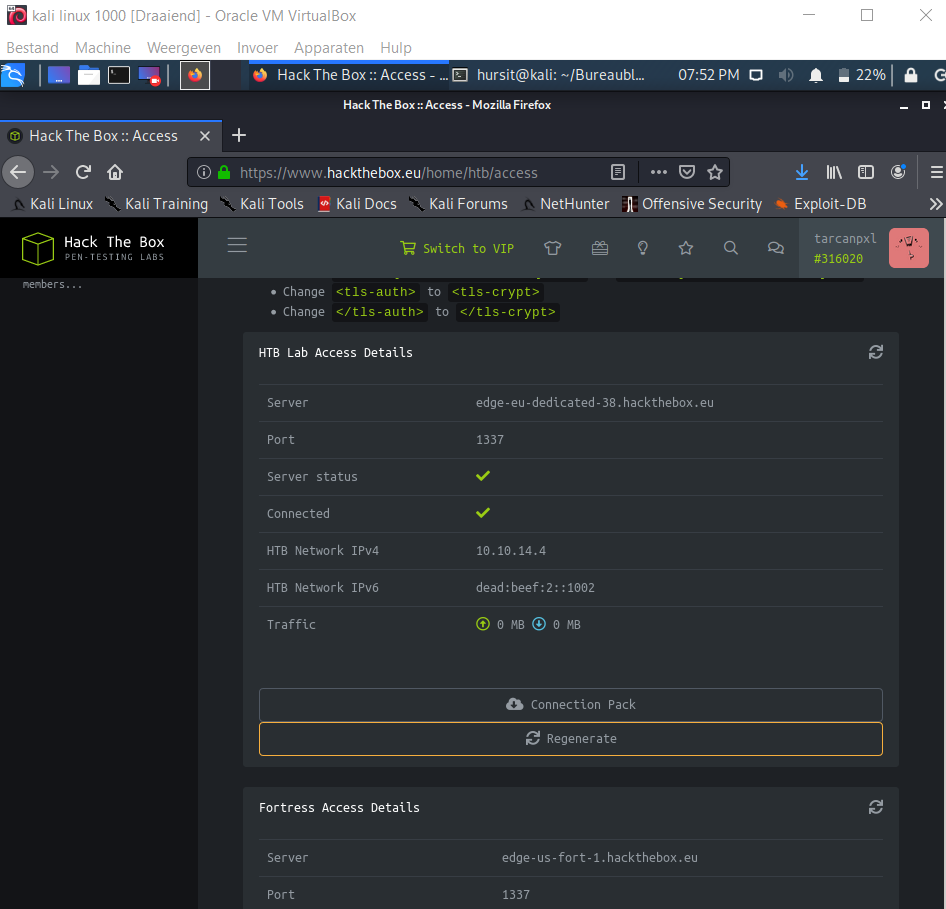
Als we dit nu in het inputfield plaatsen op hack the box dan zien we dat de challange compleet is.

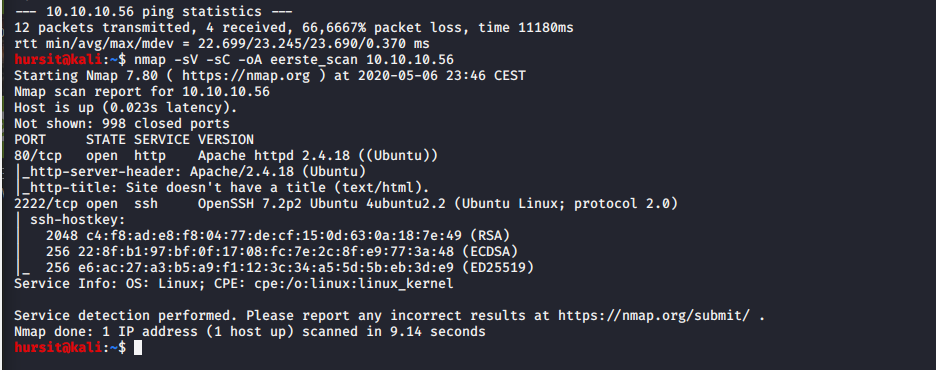




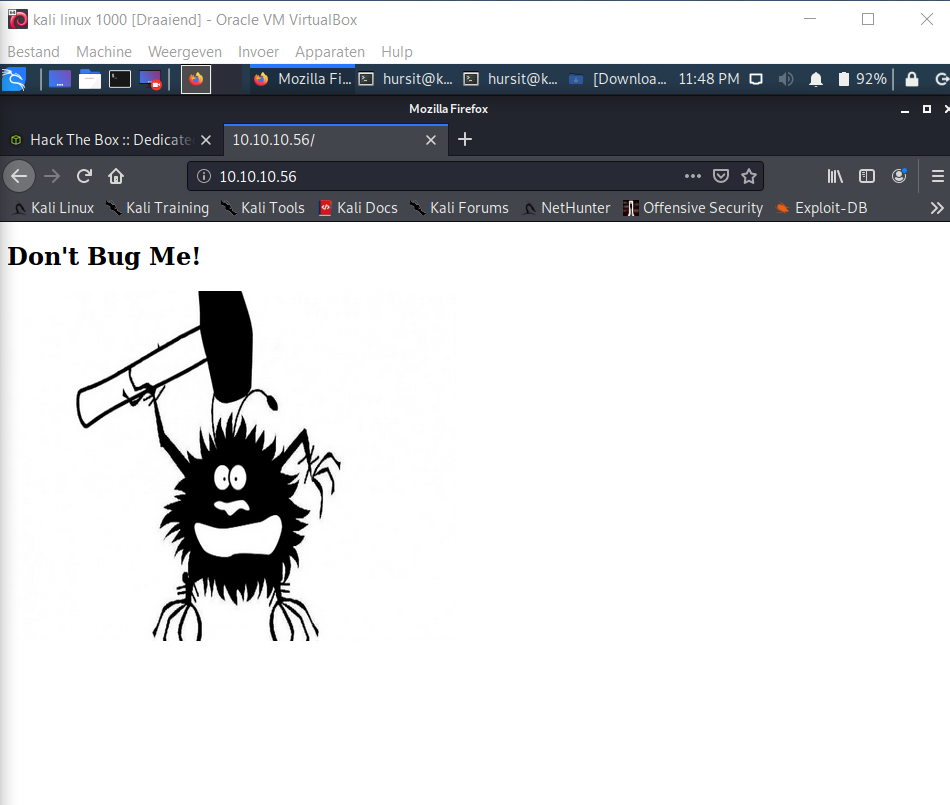
Nu alle OSINT challanges gedaan zijn kunnen we beginnen met het labo gedeelte. We gaan beginnen met ‘Shocker’. 

De eerste stap is om verbinding te maken met het netwerk via vpn. (dit staat uitgebreid uitgelegd bij een guide op Hack The Box zelf.

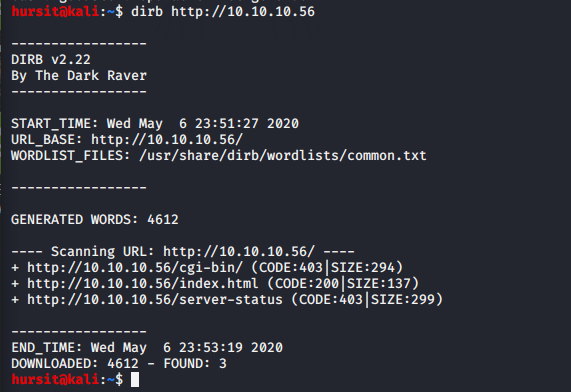




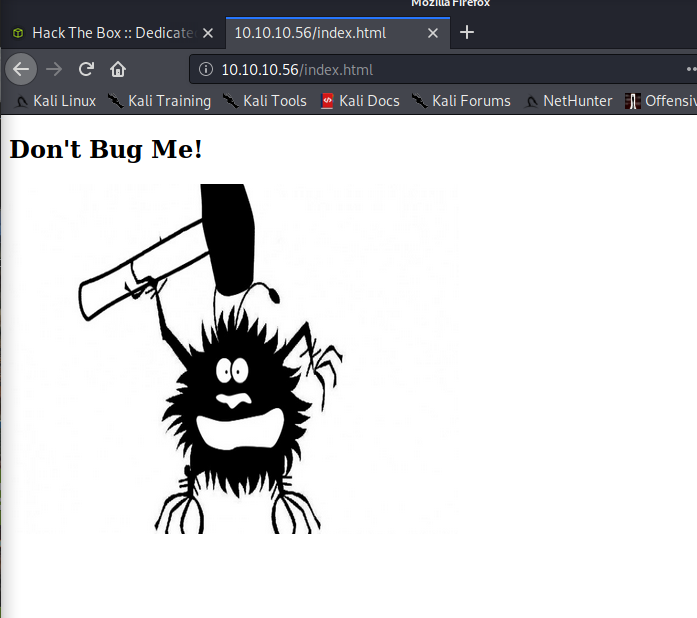
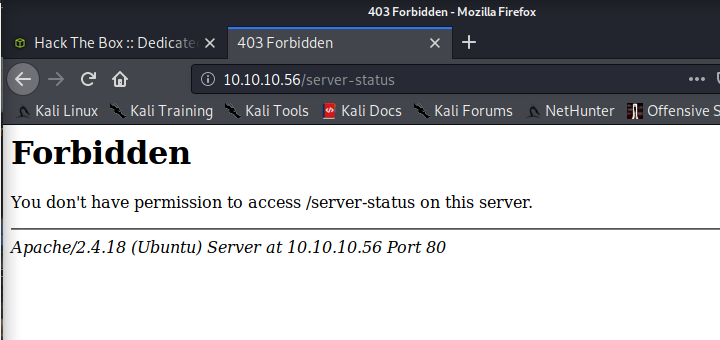
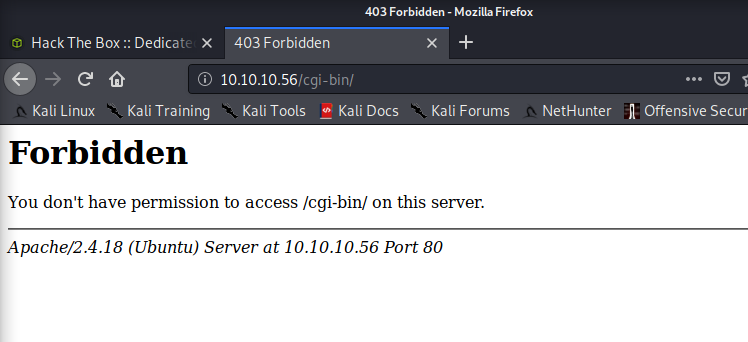
Nu gaan we het commando nmap uitvoeren om te zien welke poorten we kunnen gebruiken bij onze aanval. We zien poort 80 en 2222. Als we gaan kijken bij dit IP-adres in onze browser dan krijgen we dit als resultaat:

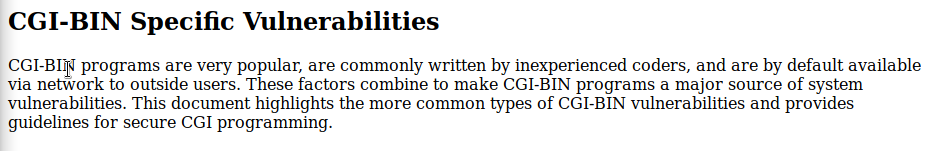


Verder is er niet veel meer te zien. We gaan nu het commando dirb gebruiken. Dirb scant een website om ons alle files terug te geven die gebruikt worden.

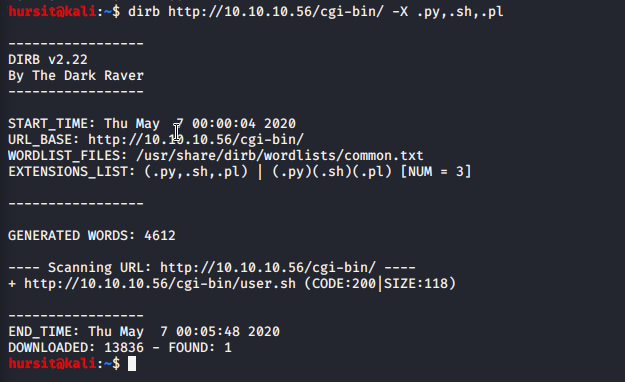


We krijgen drie files terug. En we gaan deze alle drie testen. Met wat opzoekwerk heb ik ook meegekregen dat index.html en server-status heel normale files zijn, maar dat cgi-bin een speciale file is. In volgende afbeeldingen een definitie waarin alles duidelijk staat verteld.

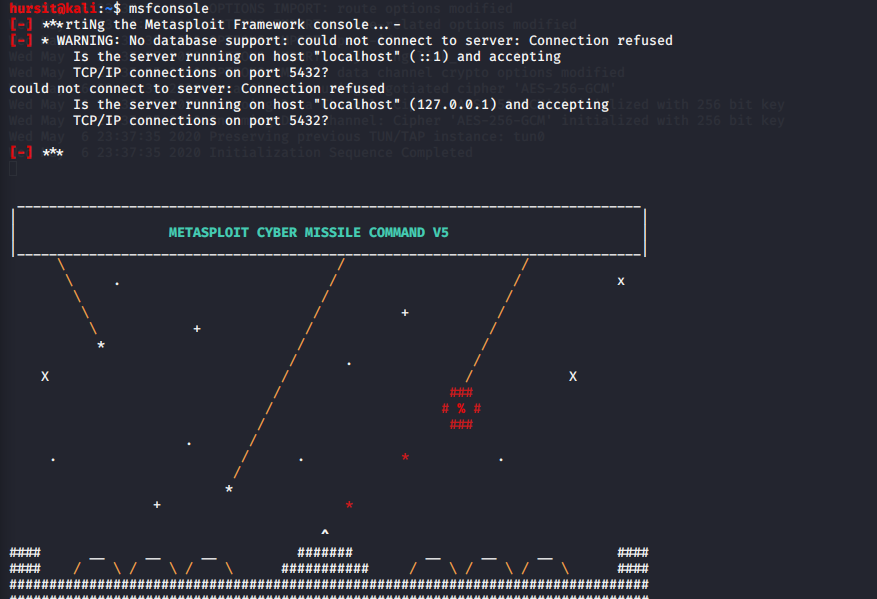




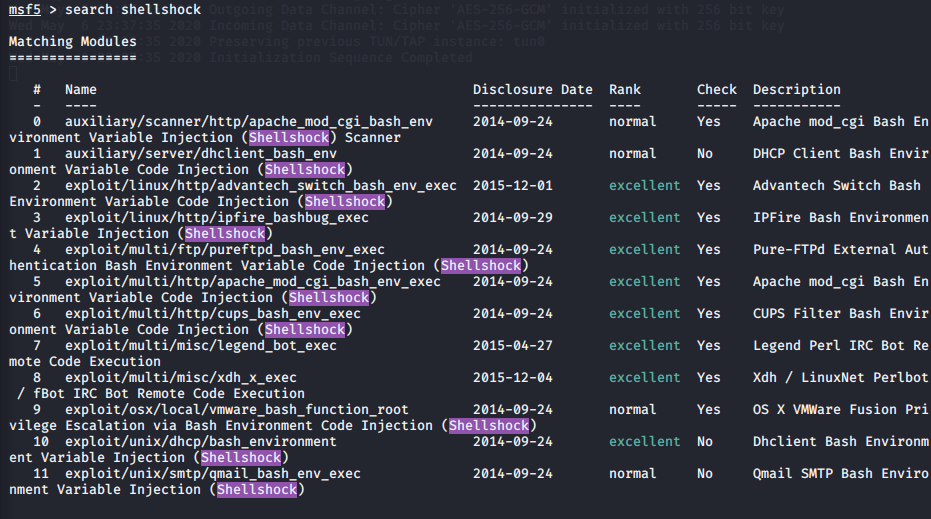
Als we meer info verzamelen over cgi-bin dan zien we dat het vaak gaat over files met extensies zoals: .py, .sh, .pl, etc…. Dus weer gaan we een scan uitvoeren maar deze keer specifiek op deze extensies.

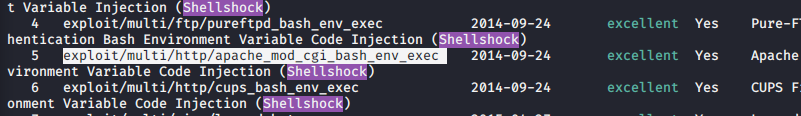


We zien dat er een user.sh file is. Nu e dit ook weten gaan we weer gebruik maken van msfconsole.

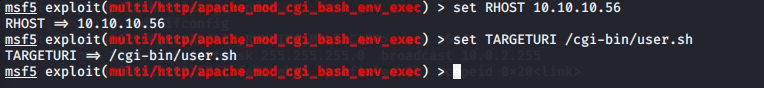


We gaan de shellshock exploit gebruiken, deze info heb ik opgezocht en bij de tips kreeg ik mee dat de exploit shellshock moest zijn en dat de machine daarom ook shocker heet.

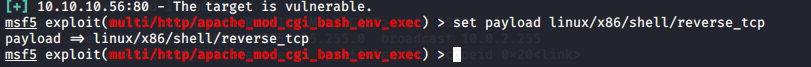




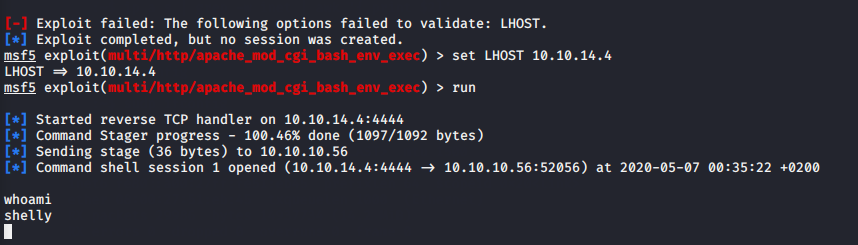
We gaan het pad op de bovenstaande afbeelding gebruiken. Nu we deze exploit gebruiken moeten we onze parameters meegeven. Een RHOST, LHOST, Payload (zoals bij de c requirements), maar deze keer komt er ook een TARGETURI bij.



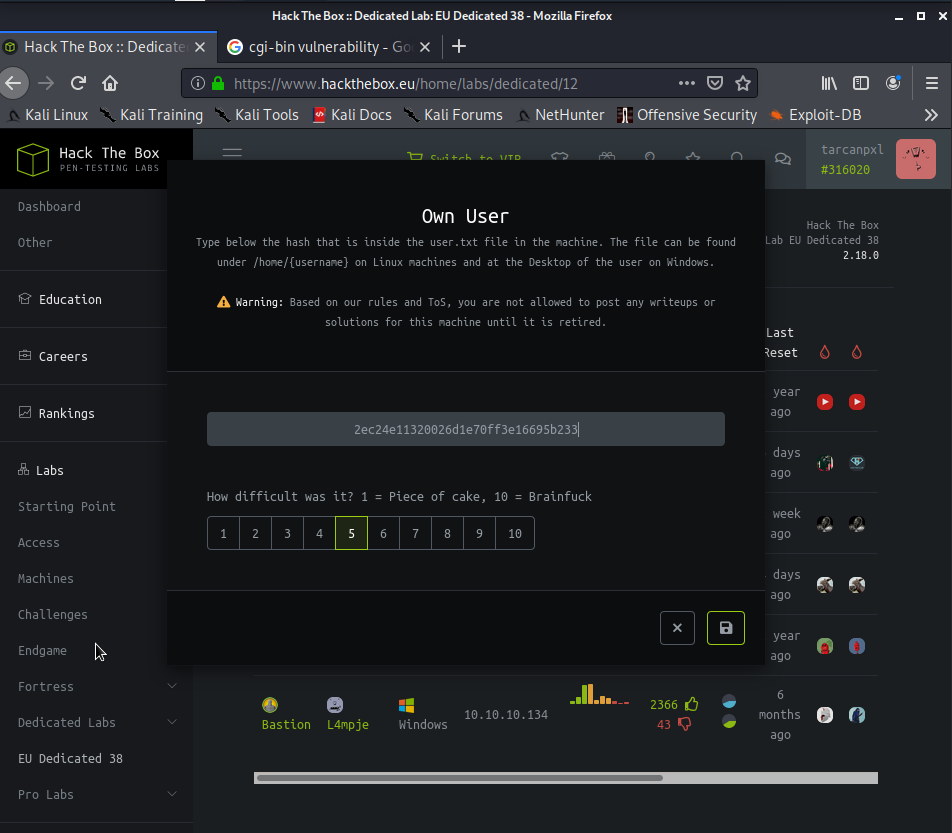




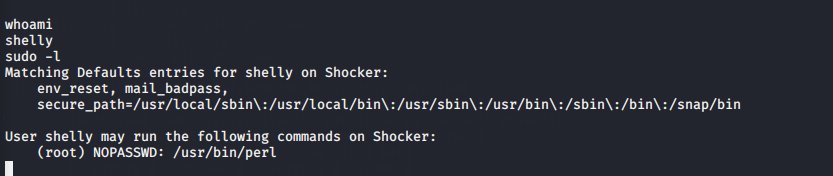
Nu alles is ingevuld kunnen we ‘run’ typen om de exploit uit te voeren.



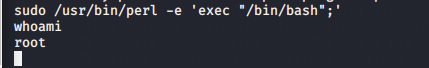
Als alles goed verloopt krijgen we nu een open sessie, als we nu ‘whoami’ typen dan zien we dat we ‘shelly’ zijn. Als we in de homefolder van ‘Shelly’ gaan kijken dan zien we het bestand user.txt. Met daarin de flag voor Own User op Hack The Box.



Nu hebben we nog root access nodig, hiervoor gaan we de machtigingen van de gebruiker shelly bekijken.



We zien dat de user ‘shelly’ in /usr/bin/perl kan zonder een wachtwoord te moeten gebruiken. Dit gaan we doen.



Nadat we hierin zijn en we typen weer ‘whoami’ dan zien we dat we root zijn. In de home folder van root zien we zoals bij Shelly een bestand dat root.txt noemt, als we dit openen krijgen we de flag voor Own System.

