***PE Red Team: Frank & Herbert (2ster)***

Task 1.1

Er wordt gevraagd op welke poort Frank zijn webpagina heeft. We moeten hiervoor de juiste poort vinden dus weten we dat we de tool nmap hiervoor kunnen gebruiken.

Dus hebben we het ipadres van Frank & Herb hun app door nmap laten scannen.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hieruit blijkt dat er 3 poorten gebruikt worden:

22 voor ssh verbinding

3000 voor ppp

31337 voor http

Omdat http voor website gebruikt wordt is dit de poort die Frank voor zijn webpagina gebruikt.

Task 1.2:

Er wordt gevraagd om te zoeken wat Frank beschikbaar heeft gelaten op zijn website.

Probleem:

1. Hoe vind je beschikbare webbestanden?

Oplossing:

1. We hebben gegooglet om te kijken met welke bestanden je verborgen web bestanden kan terugvinden.

Afbeelding met tekst, schermafbeelding, zwart, scherm

Automatisch gegenereerde beschrijving

Dit gaf ons UrlBuster als resultaat.  
Hierna zijn we gaan kijken hoe UrlBuster werkt en hoe te gebruiken 🡪 het lukte ons niet onmiddellijk via UrlBuster 🡪 alternatieven gegooglet:

Een volgende oplossing was DirBuster, na het installeren van DirBuster vonden we uitleg om de <url:poort> te scannen. Dus in ons geval <http://10.10.217.45:31337>. Dit zou 43553999 dagen duren dus hebben we afgebroken en gekeken wat we nog konden doen.

Na wat zoekwerk vonden we een kali linux tool dirsearch wat opdezelfde manier zou werken als DirBuster.

Dus hebben we onze <url:poort> ook eens door dirsearch gehaald.

Dit geeft al vrij snel resultaten weer waarvan 2 met een 200 response.

Afbeelding met tekst, schermafbeelding, computer, zilver

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

In de hint viel mij onmiddellijk op “git you here”. Was dit een spellingsfout?  
Maar na onze dirsearch hadden we een 200 response van /.git-credentials.

De website van Frank was 10.10.217.45:31337 dus hebben we eens geprobeerd om /.git-credentials erachter toe te voegen en dit gaf ons een pop-up om een bestandje te saven.

Afbeelding met tekst, schermafbeelding, monitor, zwart

Automatisch gegenereerde beschrijving

We hebben een bestand gevonden in .git-credentials. Wat ons verteld dat .git-credentials is bloodgesteld.

Task 1.3:

Het eerder gevonden bestand gaf ons “http://frank:f%40an3-1s-E337%21%21@192.168.100.50”.

Dit lijkt enorm om hoe je een ssh verbinding maakt (ssh username@ip-address). Wij veronderstellen dat dit gaat zijn: [frank@192.168.100.50](mailto:frank@192.168.100.50) met zijn password. Ook omdat er bij de nmap search een open poort 22 voor ssh verbinding stond.

De volledige tekst die wij kregen staat in url vorm.

Door in google “url code” in te geven kregen we als eerste een online rul enocode/decode website.

Afbeelding met tekst, schermafbeelding, monitor, zwart

Automatisch gegenereerde beschrijving

We hebben hier de tekst eens ingeven en dit gaf ons volgende resultaat:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

We hebben dan ssh verbinding proberen te maken met [frank@192.168.100.50](mailto:frank@192.168.100.50) wat niet lukte.  
Maar zijn website zit op 10.10.217.45 dus hebben hier ssh verbinding proberen mee te maken en dat is gelukt.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Er wordt gevraagd wat de user.txt flag is.

Na een ls hebben we gezien dat Frank een bestandje heeft user.txt. Om te kijken wat erin staat hebben we een cat hiervan gedaan en kregen we het gevraagde resultaat.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Task 1.4:

Probleem:

1. Waar moeten we beginnen?

Oplossing:

1. Laten we eerst eens kijken wie en wat we zijn:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hier komen de microk8s van pas waar de inleiding van deze oefening over sprak.

Wat zijn micork8s:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Waarvoor worden ze gebruikt:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hebben microK8s ook exploits?

Afbeelding met tekst, schermafbeelding, zwart, scherm

Automatisch gegenereerde beschrijving

Hier vinden we dat er een exploit is die een gebruiker met weinig privileges toch root kan maken.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hier staat een heel Proof-Of-Concept exploit uitgelegd. Dus hebben we deze stappen maar eens gevolgd om te kijken wat dit ons kan opleveren.

Eerst moesten we een pod.yaml file aanmaken met volgende gegevens:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Nadien moesten we deze file toepassen dmv:

microk8s.kubectl apply -f pod.yaml 🡪 dit gaf ons een foutmelding of the juiste host of poort gebruikt was.



We hebben dit moeten opzoeken en de oplossing is dat je de pod.yaml file moet toepassen op de image die al draait en dit kan je vinden door:

Afbeelding met tekst

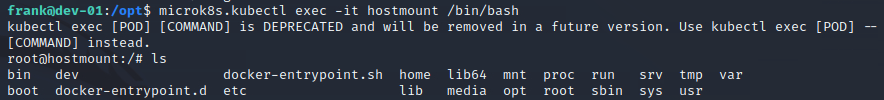
Automatisch gegenereerde beschrijving

In onze situatie gaan we de image op van localhost gebruiken. Dus passen we in onze pod.yaml file de image: ubuntu:latest aan naar localhost:32000/bsnginx en proberen het microk8s.kubectl apply -f pod.yaml commando nog eens.

Nu zien we dat de pod/hostmount is gelukt



De volgende stap die we moesten volgen was een nieuwe bash openen en hebben we hier al eens een ls gedaan:



Omdat in de pod.yaml het volume “root” hebben genoemd en het mountPath: /opt/root is gaan we cd’en naar opt/root om dan de root folder te raadplegen:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hier hebben we een ls gedaan en vonden we het bestand root.txt.

Door te kijken wat er in dit bestand zit door cat root.txt hebben we de gevraagde flag gevonden.

Afbeelding met tekst, schermafbeelding, monitor

Automatisch gegenereerde beschrijving