***PE Blue Team: Juicy Details (2ster)***

Task1:

Are you ready?

I am ready!

Task2

2.1:

De hint zegt dat we in de access.log moesten zoeken.

We zijn door heel de file gegaan (van boven naar onder) en alle tools die er gebruikt zijn genoteerd.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Daarna opgezocht via google welke van deze tools door attackers gebruikt worden, deze vergeleken met de resultaten uit de file en zo de oplossing gevonden. Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijvingAfbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

2.2:

Probleem:

1. Wat is een endpoint?

Oplossing:

1. Via google opgezocht wat een endpoint is. In een API worden deze gecategoriseerd als SOAP of REST. (REST gebruikt ook GET, POST, PUT en DELETE)

Omdat bruteforce attacks vaak gepaard gaan met dictionary attacks (uit de vorige vraag blijkt dat hydra hier gebruik van maakt) zijn we in de file access.log gaan kijken waar hydra voor gebruikt werd.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

2.3:

Uit vraag 1 hebben we geleerd dat sqlmap gebruikt maakt van sql injection. Dus zijn we gaan kijken naar de logs van sqlmap:



2.4:

In de resultaten van vorige vraag zien we dat er na “search” volgende wordt meegegeven -> ?q=

Hieruit kan je afleiden dat de parameter “q” gebruikt wordt.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

2.5:

Retrieving files doet ons denken aan files downloaden/overzetten van 1 plaats naar een andere zoals bij bv FileZille. Dit heeft een ftp protocol om de uitwisseling te vergemakkelijken.

We hebben eens gekeken of we dit terug vonden in de file access.log.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Task3

3.1:

De hint zegt dat we moeten gaan kijken daar waar klanten meestal commentaar over een winkel website kunnen achterlaten, dus wij dachten aan een review schrijven.

Door in de file access.log te kijken of we ergens het trefwoord “review” vonden stond dit bij “products”

Afbeelding met tekst

Automatisch gegenereerde beschrijving

3.2:

In de file kan je zien dat “hydra” probeert in te loggen door de POST /rest/user/login -> brute force. Deze geven response codes 401 -> unauthorized en 500 -> generic error response. Maar 1 van deze pogingen geef een response code 200 -> succeeded terug

Afbeelding met tekst

Automatisch gegenereerde beschrijvingAfbeelding met tekst

Automatisch gegenereerde beschrijving

3.3:

In access.log zien we veel GET /rest/products/search?=q….

Op een bepaald ogenblik is een ene GET met %20SELECT%20id,%20email,%20password in de code waaruit we kunnen afleiden dat de attacker probeert het email en password van de user te verkrijgen.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

3.4:

Zals de vraag aangeeft moeten we gaan kijken naar de ftp uit vraag 5 van Task2.

Bij deze resultaten zie je nog de details www-data.bak en coupons\_2013.md.bak staan waaruit je kan afleiden dat de attacker deze files probeerde te downloaden.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

3.5:

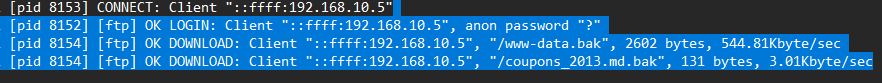
We hebben hier niets van gevonden in de file access.log dus hebben we eens gekeken in auth.log waar we enkel authenticatie gegevens terugvonden van user en wachtwoord en vonden we niets terug over de files uit de vorige vraag.

In de file vsftpd.log kan je volgende code zien [anonymous] FAIL LOGIN: client waaruit we kunnen opmaken dat de attacker probeert om in te loggen met username anonymous.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Nadat dit gelukt is zie je dat er terug gebruikt wordt gemaakt van ftp voor de bestanden uit vorige vraag.



3.6:

In de file auth.log zie je op de eerste regel onmiddellijk Failed password for www-data from 192.168.10.5 port 40066 ssh2. Waaruit we kunnen afleiden dat het ingegeven passwoord voor www-data van ip adres 192.168.10.5 via poort 40066 over ssh2 mislukt is. Dus de attacker probeert het paswoord van account www-data via ssh verbinding te verkrijgen.

Afbeelding met tekst, oranje

Automatisch gegenereerde beschrijving