PEN test 1 - CentOS - SSH

Een PEN test is een penetratietest. Een test om te kijken en te controleren of je ergens binnen kunt komen. Dat kan een file server zijn maar dat kan ook een web server zijn. We zelf een PEN test uitvoeren op onze eigen web site en we gaan de website daarna veiliger maken. In deze les gaan we een server inrichten als voorbereiding op de PEN test.

Het uitvoeren van de PEN deel van het examen Veilig programmeren.

Overzicht

Testen op XAMP heeft weinig zin, omdat dat een afgeschermde development omgeving is en een development omgeving is niet veilig (zie opgave 1).

We gaan dus een productieomgeving inrichten daarvoor gebruiken we VMWare. Dit lijkt heel erg op een echte productie machine. Als je nog van plan bent om zelf een productieserver in te richten, let dan goed op want de stappen die we gaan nemen zijn vrijwel hetzelfde bij het inrichten van een VM.

Via VMWare gaan we een CentOS (7) Linux machine inrichten. Er zijn meerdere Linux distributies, maar CentOS is gratis en wordt veel gebruikt als (web)server.

Nadat we een Linux server hebben, gaan we deze installeren en inrichten. Hiervoor zul je ene boel moeten uitzoeken op het internet. In deze les worden alleen de stappen beschreven; je moet zelf uitzoeken en overleggen hoe het allemaal precies werkt.

Als de server is ingericht met **MariaDB**, **PHP7.x** en een **Apache** webserver dan gaan we onze eigen web applicaties installeren. Het beste is als we een PHP voorbeeld en Laravel voorbeeld kunnen gebruiken. Dan kunnen we de verschillen zien.

Met een zogenaamde Nikto scan gaan we de test uitvoeren.

Installation

Install VMWare Workstation 15.

(https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html)

New VM

Download CentOS DVD: http://isoredirect.centos.org/centos/7/isos/x86_64/

(ik heb deze lijnk gekozen: http://centos.mirror.triple-it.nl/7.7.1908/isos/x86_64/CentOS-7-x86_64-DVD-1908.iso)

Install CentOS

Start VMWare PLayer op en start en install van de ISO die je hebt gedonwload.

- Extra VMWare tools hoef je neit te downloaden als daar om wordt gevraagd.
- Taal English (Ireland)
- System Installation Destionation aangeven (op nieuwe VMWare Schijf).
- Network & Host Name selecteren en Ethernet (rechtsboven) aan zetten!
- Begin Installation
- Root password instellen (niet vergeten; opschrijven!)
- Geen user aanmaken (tijdens installatie)
- Reboot

Done

Install Software

(based on tutorials from https://www.howtoforge.com)

Eerst moeten we een repository toevoegen (dat is een soort database met software):

```
yum -y install epel-release
```

Dan gaan we een editor installeren omdat de meeste de standaard vi editor te lastig vinden.

```
yum -y install nano
```

Dan gaan we MariaDB Installeren

```
yum -y install mariadb-server mariadb
```

Datbase opstarten en zorgen dat die bij een reboot weer automatisch wordt gerestart.

```
systemctl start mariadb.service
systemctl enable mariadb.service
```

Nu moeten we een root wachtwoord voor de SQL server instellen.

```
mysql_secure_installation
```

Install Apache Webserver.

```
yum -y install httpd
```

Start de webserver en zorg dat die bij een reboot weer automatisch wordt gerestart

```
systemctl start httpd.service
systemctl enable httpd.service
```

Zet een hostname voor je Appache Server

```
nano /etc/httpd/conf/httpd.conf
```

En plaats deze regel. De regel staat al in de file maar er staat een # voor waardoor de regel in commentaar staat. Haal dat # weg.

Zet firewall for http en https open.

```
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Check wat je ip address is (zoek zelf even uit hoe) en controleer of je browser de standaard Apache web pagina kan vinden op je nieuwe server.

Nu gaan we PHP installeren, eerst de juiste repo toevoegen, alle software updaten en de installer (YUM) updaten.

```
rpm -Uvh http://rpms.remirepo.net/enterprise/remi-release-7.rpm
yum -y install yum-utils
yum update
```

Install PHP 7.3

```
yum-config-manager --enable remi-php73
yum -y install php php-opcache
```

En restart de web server.

```
service httpd restart
```

De docuement root is `/var/www/html`

Zet daar een klein PHP scripje neer om te controleren of de PHP engine werkt.

Done!

Website maken

Een (niet-Laravel) web site kan je nu maken door de in de document root directory te maken en daar in een web site te plaatsen. Gebruik een van de websites die we eerder hadden gemaakt en cotnroleer of die werkt.

Voor het aanmaken van een Laravel website is het handig dat we grote heoveelheden files tussen onze Laptop en de VM kunnen kopieren, dat doen we later.

Installeer MobaXterm (of Putty)

We hebben tot nu toe rechtstreeks op de VM gewerkt Dit is alsof we in een datacentrum staan en rechstreeks op onze server werken. Zo werkt het bij een niet-VM natuurlijk niet. We moeten dan remote aanloggen en dat doen we met een SSH client. Download MobaXterm en maak via SSH een verbinding met he VM die in de achtergrond natuurlijk wel draait.

Omgeving veilig(er) maken

Er is een aantal zaken die we kunnen regelen om onze omgeving veiliger te maken:

- Als je via een SSH client aanlogt op je (VM) server dan moet je een password gebruiken. Enerzijds wil je je password heel lang maken en anderzijds moet je het telkens intypen en wil je het niet te lang maken. Om dit te voorkomen kun je SSH keys opzetten. Dit werkt via PPK (Public Key Infra Structuur). Weet je nog van dat hangslotje hoe dat werkt? We gaan in MobaXterm een SSH key pair maken. Je plaatst je public key op de server en houd je private key op je laptop. Het opzetten van SSH keys tussen een Windows machine en een LInux machien is redelijk complex en daarom gaan we dit in de les samen doen.
  Zonder deze stap kun je wel gewoon door met de rest van deze les.

- Eingenlijk zou je nooit met root (Super User - mag alles!) moeten aanloggen. Sterker: je kan je server zo instellen dat je nooit rechtstreeks met root kan inloggen, maar alleen via een ander account. Het is een goed gebruik om root niet of alleen in noodgevallen te genbruiken. We moeten dus een eigen user voro onszelf maken.

- Zoek nu op hoe je in de `/etc/sudoers` file je nieuwe gebruiker de rechten kan geven om zichzelf super user te maken. Op die manier kun jij ook alles. Als je iets niet kan dan typ je er sudo (Super User Do) voor en hoppa, je bent voor dat ene commando root.

- In de webserver directory gaan we de rechten nu zo instellen dat we met onze 'gewone' user files kunnen plaatsen en kunnen aanpassen. Natuurlijk moet je hier *max* vervangen in de user die je zelff hebt aangemaakt.

```
sudo chown max:apache /var/www/html/
```

- SSH gaat standaard over poort 22. Als je een domein hebt dan duurt het vaak niet langer dan een paar weken en dan zijn er 1000+ hackers die proberen een SSH verbinding op te zetten naar jowu server. In de VM omgeving heb je hier natuurlijk geen last van. Door SSH over een 'geheime' poort plaatst te laten vinden houd je een boel gelegenheids hackers buiten de deur. Zoek uit hoe dat werkt en stel dat in op je VM. Zorg er dan ook voor dat je SSH client ook via de andere alternatieve poort gaat (dit is opgave 6).

Opgaven

1. Zorg ervoor dat je webserver met PHP draait op je VM. Hierboven staat beschreven hoe je dat moet doen.
   Maak een schermafdruk waarop je URL te zien is en voer een PHP scripje uit dat jouw naam op het scherm zet (in de brwoser).

2. Noem een aantal zaken waar je aan zou moeten denken als je een web site vanuit jouw XAMPP development omgeving in productie zou willen zetten. Wat moet je veranderen/aanpassen (denk aan alles wat we tot nu gedaan hebben)?

3. Noem twee goede redenen waarom je zeker in een omgeving met meerdere system managers het root account nooit (rechtstreeks) wilt gebruiken.

4. Waar staat SSH voor?

5. Waarom heb je in een VM omgeving geen last van hackers die proberen via poort 22 een SSH verbinding op te zetten?

6. Zorg ervoor dat het SSH verkeer over een andere dan poort 22 plaats vind. Zoek zelf op internet uit hoe dat werkt?

7. Hoe zou jij als heacker proberen binnen te komen via SSH; wat zou je doen/proberen?

8. Stel iemand hacked jouw (VM) server en steelt jouw key uit de file `authorized_keys`. Wat kan de hacker nu? Kan die in alle servers komen waar jij via dit key/pair toegang tot hebt? Leg uit hoe en waarom.

9. Met het commando `sudo su` maak je jezelf root en hoef je niet telkens `sudo` in te typen. Waarom zou dit een slechte gwoonte zijn?

10. Beschrijf van de volgende Linux commando's wat ze doen en test ze uit. Geef telkens een voorbeeld.

Commando	Voorbeeld	Uitleg
cd		
mv		
rmdir		
rm		
mkdir		
ll (of ls-la)		
history	niet nodig	
exit	niet nodig	

--

Revision #23
Created 2019-12-01 16:35:13 UTC by Admin
Updated 2022-03-12 17:26:05 UTC by Max