Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

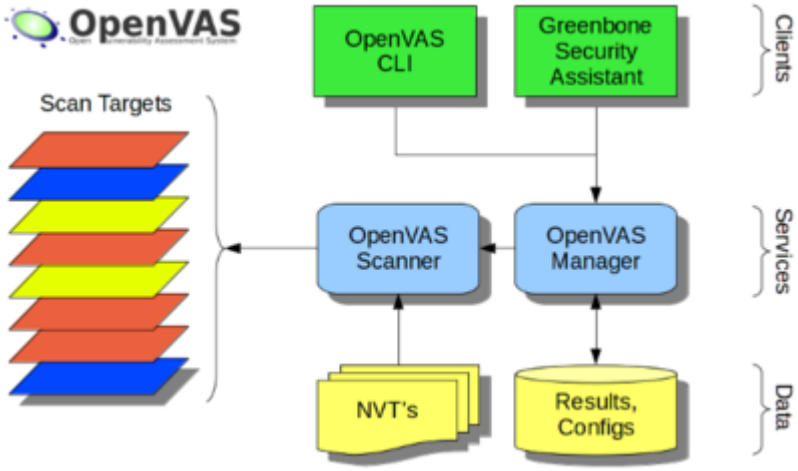
NOTA: per desgràcia, no hem pogut implementar a dins. Degut a quant estava tot instal · lat no trovaba les xarxes i els hosts.

OpenVAS: Open Vulnerability Assessment System

Es un escàner de vulnerabilitats amb totes les funcions. Les seves capacitats inclouen proves no autenticades i autenticades, diversos protocols industrials i d'Internet d'alt i baix nivell, ajust de rendiment per a exploracions a gran escala i un potent llenguatge de programació intern per implementar qualsevol tipus de prova de vulnerabilitat. L'escàner obté les proves per detectar vulnerabilitats a partir d'un canal que té un llarg historial i actualitzacions diàries.

OpenVAS ha estat desenvolupat i impulsat per l'empresa Greenbone Networks des de l'any 2006. Com a part de la família de productes de gestió de vulnerabilitats comercials Greenbone Enterprise Appliance, l'escàner forma Greenbone Vulnerability Management juntament amb altres mòduls de codi obert.

Ens va permetre escanejar objectius tan dispositius mòbils, dispositius de xarxa, PC, etc. allò que sigui que estigui connectada a la nostra xarxa. Amb el fi d'aconseguir possibles vulnerabilitats que tinguin aquestes hosts i per poder fer dues coses: - Per una banda, si som l'atacant o l'auditor, intentar explotar-les. - I si estem a l'equip de defensa, intentar defensar-los i tancar-los correctament.



Dins del panl de monitoritzacio del OpenVAS podem veure les xarxes, hosts o un grup d'IPs per poder escanjer a dispositius de xarxa, a dispositius mobils, a servidors, a PC, a aplicacion, un munt de coses.

Practica

1. Actulitzar el sistema (pot trigar una estona!).

```
sudo apt update -y && sudo apt -disupgrade -y
```

2. Aque ja si, instal · lar el paquet OpenVAS.

```
sudo apt install openvas -y
```

3. Ara passem a lo mes aburrit, esperar. Instal · lem l'aplicacio, per aixo necessitar descarregar totes les firmes per poder detectar vulnerabilitats que qualsevol sistema per exemple apache2, windows, ... En resum que trigarar un mun de hores. En el nostre cas va tarda 1 hora i mig . En un altre exemple va trigar 3 hores.

```
sudo gmv setup
```

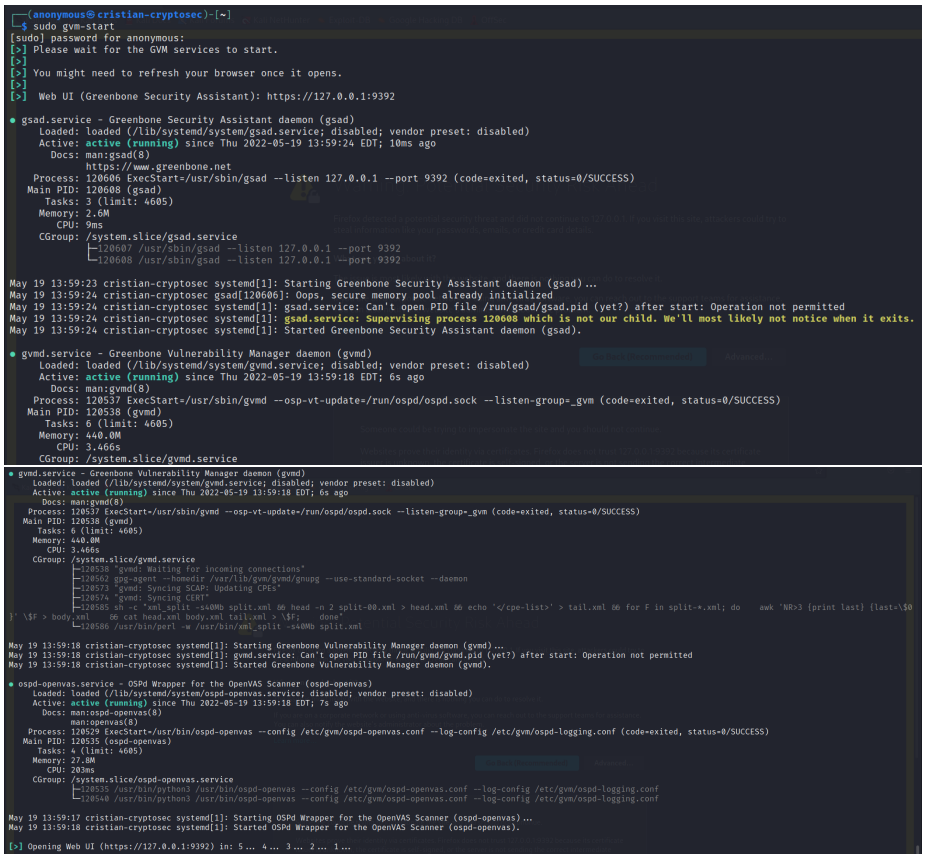
```
      2,134,519 100%  820.02kB/s    0:00:02 (xfr#19, to-chk=11/31)
dfn-cert-2016.xml
      2,640,075 100%  845.31kB/s    0:00:03 (xfr#20, to-chk=10/31)
dfn-cert-2017.xml
      3,127,997 100%  997.94kB/s    0:00:03 (xfr#21, to-chk=9/31)
dfn-cert-2018.xml
      3,535,053 100% 1002.67kB/s    0:00:03 (xfr#22, to-chk=8/31)
dfn-cert-2019.xml
      3,551,378 100%  903.87kB/s    0:00:03 (xfr#23, to-chk=7/31)
dfn-cert-2020.xml
      3,661,582 100%  819.38kB/s    0:00:04 (xfr#24, to-chk=6/31)
dfn-cert-2021.xml
      3,615,045 100%  919.83kB/s    0:00:03 (xfr#25, to-chk=5/31)
dfn-cert-2022.xml
      1,615,102 100%  693.30kB/s    0:00:02 (xfr#26, to-chk=4/31)
sha1sums
          1,532 100%    6.62kB/s    0:00:00 (xfr#27, to-chk=3/31)
sha256sums
          2,180 100%    9.42kB/s    0:00:00 (xfr#28, to-chk=2/31)
sha256sums.asc
            819 100%    3.10kB/s    0:00:00 (xfr#29, to-chk=1/31)
timestamp
             13 100%    0.05kB/s    0:00:00 (xfr#30, to-chk=0/31)

sent 685 bytes  received 85,248,941 bytes  1,008,871.31 bytes/sec
total size is 85,226,125  speedup is 1.00

[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '4967909f-733c-4151-92d0-8a1a9eccde10'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured
```

4. Un cop acabat l'instal · lacio ens donara un nom d'usuari i un password per poder entrar al panel del OpenVAS. Es important guardar-ho en un lloc segur.

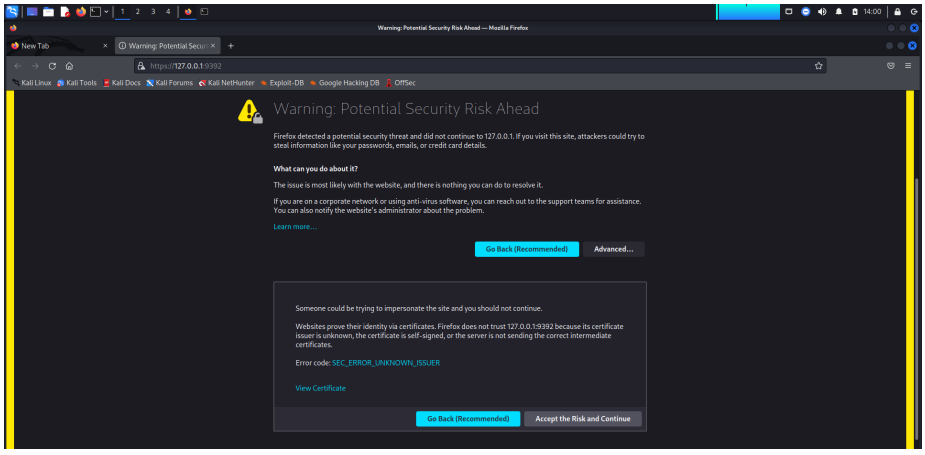
```
admin
aa6f95ca-9641-47f4-bd7d-7a5c5a56b934
```

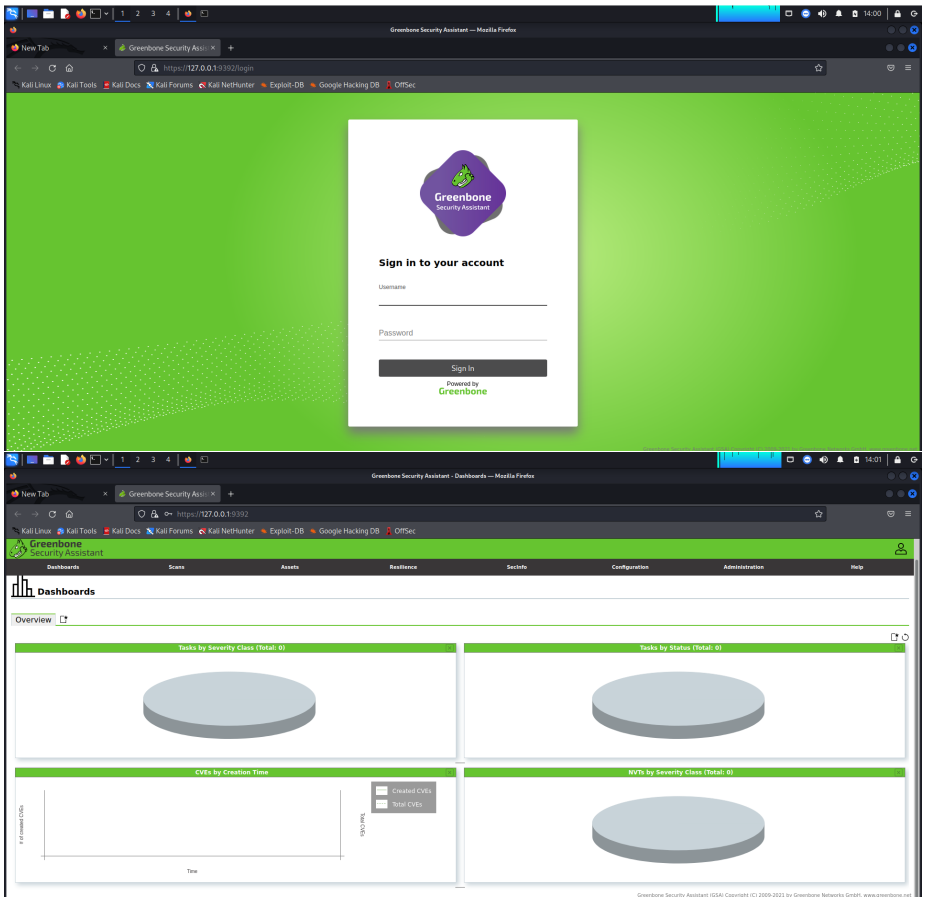
5. Primer inicem el openvas. En cas de que surti `Failed` el podem resoldre amb un `restart` o en aquest cas es un `stop` i un `star` de nou.

```
sudo gvm-start
```



6. Quant el servidor s'engega, ja ens obre un navegador. Nomes queda aceptar el certificats i iniciar sessio al OpenVAS. Ja podem observer i escanejar els dispositus/hosts/IPs de la nostra xarxa i d'altres xarxes.





Bibliografia

- https://www.youtube.com/watch?v=Sf9LKyCpgPc