# Basic Security

**Vulnerability Analysis**

## Nessus scan

### Wat is Nessus

Nessus is een kwetsbaarheidscanner om kwetsbaarheden in uw beveiliging op te sporen en op te lossen. Nessus is hier één van de beste in. Net omdat hij een rijkgevulde database heeft met CVE’s (Common Vulnerablities and Exposures), maar ook goede rapportmechanisme heeft. Dit is zeer belangrijk bij kwetsbaarheidscanners.

### Hoe Nessus gebruiken

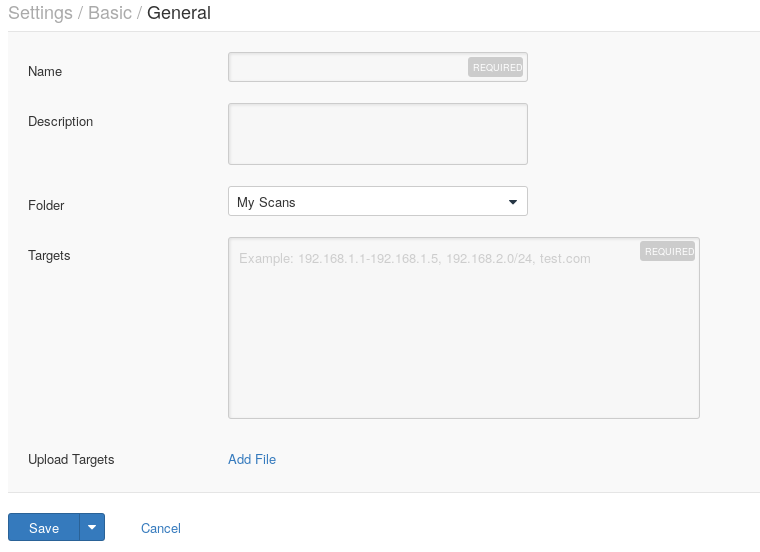
Omdat Nessus niet is voorgeïnstalleerd op Kali-Linux downloaden we een .deb bestand van hun website en installeren we met dit commando.

sudo dpkg -i nessus.deb

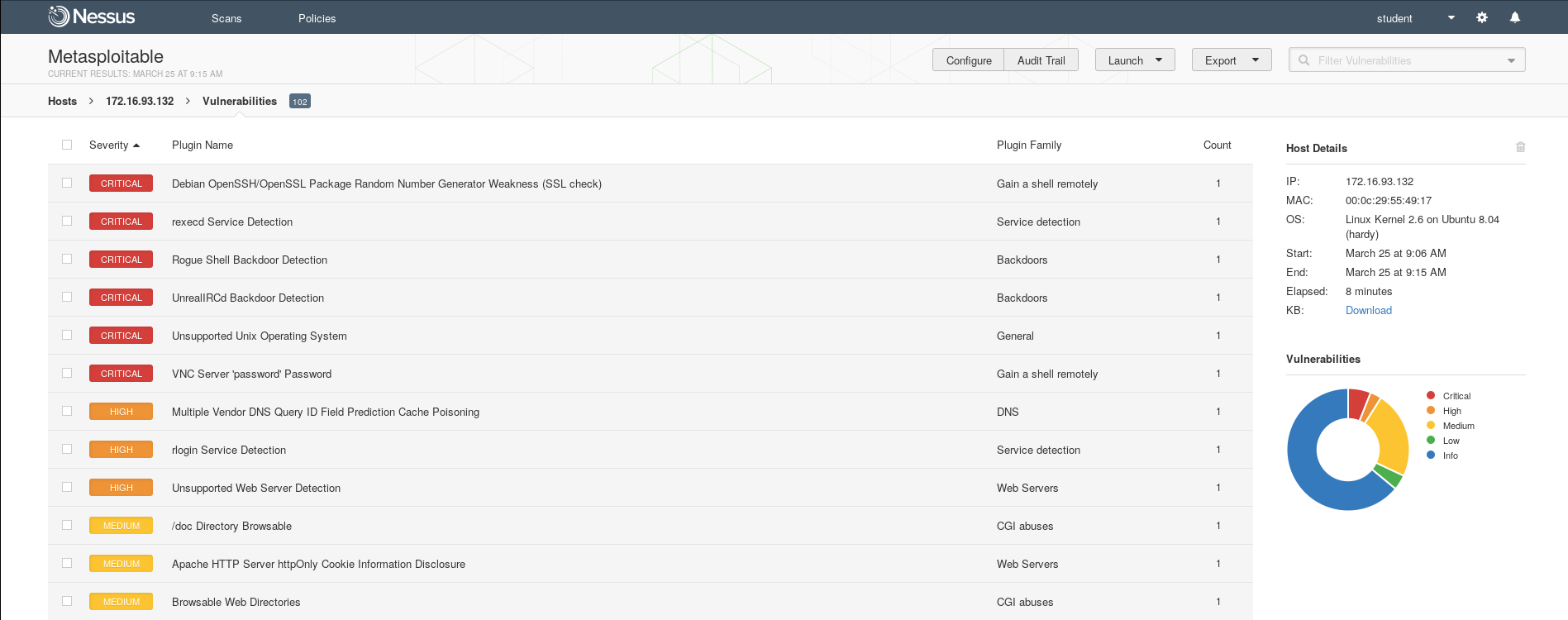
Nadat nessus geïnstalleerd is starten we deze met het volgende commando.

sudo /etc/init.d/nessusd start

Nu kunnen we in onze browser surfen naar <https://localhost:8834>. De eerste keer zal Nessus zich installeren en de nodige data downloaden. Eens dit gedaan is kunnen we beginnen met het scannen.

Eerst en vooral klikken we op ‘nieuwe scan’ en kiezen daarna voor ‘advanced scan’. We vullen daarna een naam en het IP-address in. En klikken op ‘launch’

Wanneer de scan gedaan is krijgen we een mooi overzicht van alle kwetsbaarheden en de bijhorende informatie over het systeem. Zoals welke versie en dat van de programma’s.



### Windows OS

### Metasploitable OS

|  |  |  |  |
| --- | --- | --- | --- |
| CVE | Wat | Probleem | Oplossing |
| CVE-1999-0678 | ServerRoot is de root folder waar documentatie terug te vinden is | Door een configuratie fout kan iedereen van buiten af aan de documentatie | Verwijs de serverroot naar /etc/httpd. Dit is de standaard configuratie. |
| CVE-1999-0618 | rexecd of remote execution service loop op poort 512 en zorgt ervoor dat een gebruiker van op afstand commandos kan sturen naar de OS.  Hiervoor moet de gebruiker zijn username en wachtwoord meegeven. | Het wachtwoord wordt niet geëncrypteerd bij het sturen naar de OS.  De service vertrouwd sommige hosts en IPs blindelings | De rexecd of remote execution service uitzetten en de Firewall configureren zodat TCP over poort 512 niet mogelijk is |
| CVE-1999-0651 | rlogin of remote login is een nuttige software voor linux waarbij een gebruiker over een netwerk kan inloggen op een andere computer | Het wachtwoord wordt niet geëncrypteerd bij het sturen naar de OS.  Mogelijkheid om authenticatie te omzeilen | Verwijder de 'login' lijn in /etc/inetd.conf en herstart het proces  Deactiveer de functie en gebruik SSH |
| CVE-2008-0166 | OpenSSL biedt een versleutelde transportlaag bovenop de normale. | Er wordt een verouderde versie van OpenSSL gebruikt. Deze versie genereerd voorspelbare nummers waardoor het gemakkelijk wordt voor een hacker om dit te "brute forcen". | OpenSSL updaten naar de nieuwste versie. |
| CVE-2010-2075 | UnrealIRCD is een open source IRC server. IRC (Internet Relay Chat) is een application layer protocol in vorm van chat over het internet. | Deze versie bevat een Trojan Horse in het bestand: DEBUG3\_DOLOG\_SYSTEM. Hierdoor kunnen hackers commando's uitvoeren. | UnrealIRCd van de officiele site downloaden en installeren |

## OpenVAS

### Wat is OpenVAS

OpenVAS is net als Nessus een kwetsbaarheidscanner. OpenVas is tegensteld van Nessus gratis en open-source.

### Hoe OpenVAS gebruiken

Ook OpenVAS is nog niet voorgeïnstalleerd op Kali-Linux. We kunnen dit installeren door het volgende commando in te geven.

sudo apt-get openvas

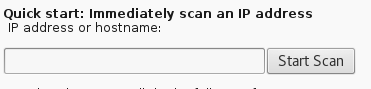
Wanneer OpenVAS geïnstalleerd is moeten we deze nog configureren, dit kan eventjes duren.

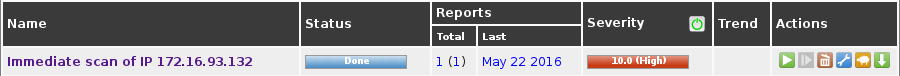
sudo openvas-setup

Daarna kunnen we deze starten met:

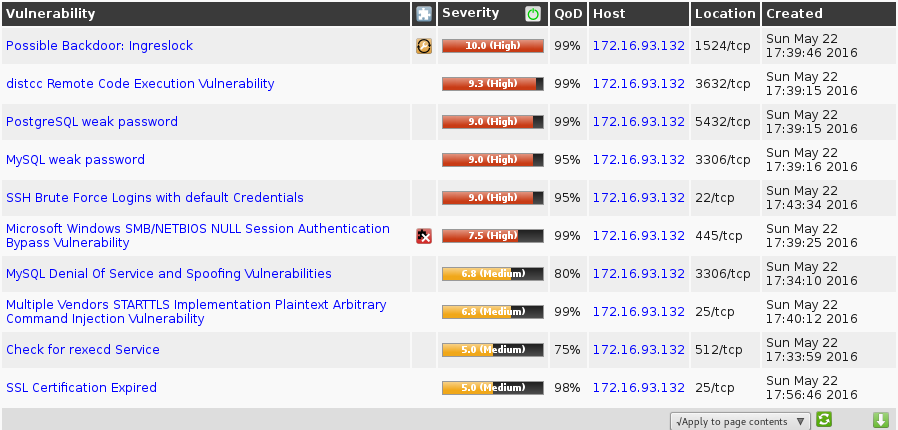
sudo openvas-start

In de browser surfen we dan naar <https://127.0.0.1:9392> . We kunnen nu beginnen met scannen door een IP-address in te geven.

Het IP-address wordt dan onmiddelijk gescand.



Wanneer de scan gedaan is kunnen we alle kwetsbaarheden bekijken.



### Metasploitable OS

We bespreken kort de 3 gevaarlijkste kwetsbaarheden op Metasploitable OS volgens OpenVAS

1. Possible Backdoor: Ingreslock  
   Er is een ‘backdoor’ gevonden waardoor hackers kunnen binnen raken en het systeem overnemen. Op dit moment word er nog naar een oplossing gezocht.
2. Distcc remote code execution  
   Wanneer distcc niet goed is geconfigureerd kunnen er commando’s worden uitgevoerd. Zonder dat deze commando’s worden gecontroleerd. Dit kan opgelost worden door distcc te configureren.
3. PostgreSQL weak password  
   PostgreSQL gebruikt het standaard wachtwoord ‘postgres’. Dit is simpel op te lossen door het wachtwoord te veranderen.

## Nessus VS OpenVAS

Welke is nu de beste kwetsbaarheiscanner?   
Eerst en vooral moeten we er wel bijvertellen dat er gewerkt is met Nessus-Home, aangezien we het niet zagen zitten om er een kleine €2000 aan uit te geven. Dit wil dan wel zeggen dat dit niet de volledige Nessus ‘experience’ geeft. Maar toch waren we onder de indruk over Nessus-Home.

Als we naar het uiterlijk kijken loopt OpenVAS enkele stappen achter Nessus. Dit is dan wel te verwachten aangezien OpenVAS gratis is.

Maar om eerlijk te zijn hebben we niet veel aan wat mooie kleuren en een leuk letter-type. Het is natuurlijk altijd fijner om naar te kijken maar dat alleen is niet voldoende om de betere kwetsbaarheidscanner te zijn.

Wat het scannen betreft. Het vinden van de kwetsbaarheden in ons systeem deed ook hier Nessus het beter dan OpenVAS. Nessus vond 6 ‘critical’, 3 ‘high’, 23 ‘medium’ en 4 ‘low’ kwetsbaarheden. En heel wat informatie over de versies van verschillende programma’s wat ook belangrijk kan zijn voor een hacker. OpenVAS hier in tegen vond 6 ‘high’, 7 ‘medium’, en 2 ‘low’ kwetsbaarheden. Er werd ook heel wat maar informatie gevonden maar niet zo veel als Nessus.

Er was ook niet alleen een verschil tussen het aantal gevonden kwetsbaarheden maar ook in het niveau. Wat bij OpenVAS als hoog werd aanschouwd, stond bij Nessus minder hoog en omgekeerd. Als we hun rapporten vergelijken zien we ook dat Nessus meer informatie geeft over de kwetsbaarheid.

Onze conclusie is dan ook vanzelf sprekend. Ookal gebruikten we niet de volledige versie van Nessus kregen we wel het beste resultaat. We kregen niet alleen meer kwetsbaarheden maar ook een beter rapport.

## Armitage

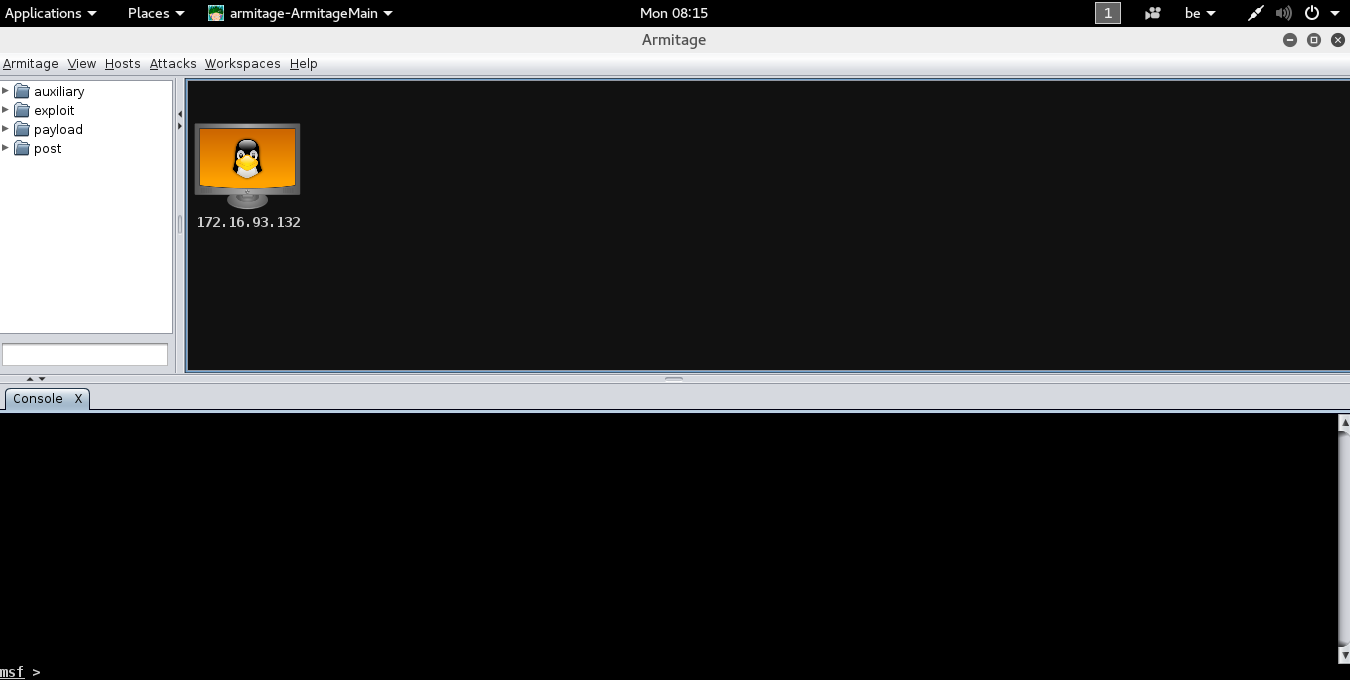
### Wat is Armitage

Armitage is een grafische management tool voor cyberaanvallen dat het metasploitframework hiervoor gebruikt. Het toont de kwetsbaarheden in een systeem en hoe deze misbruikt kunnen worden. Armitage wordt daarom dus gebruikt door security professionals om hun systeem beter te kunnen beveiligen tegen deze cyberaanvallen.

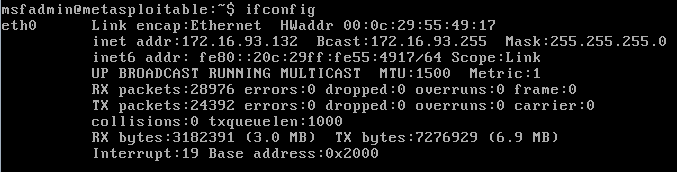
### Hoe Armitage gebruiken

Om te beginnen starten we Kali-Linux op en openen we Armitage. Wanneer er geen verbinding kan gemaakt worden met de database voeren we het volgende commando uit:

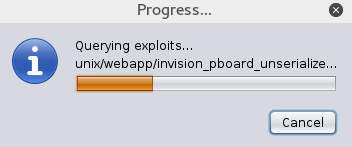
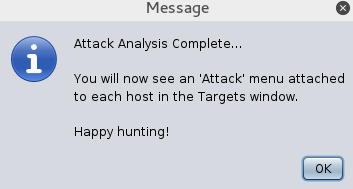
Sudo /etc/init.d/postgresql start



Nadat Armitage is opgestart voegen we een nieuwe host toe. Door op ‘Hosts’ te klikken en daarna ‘Add hosts’. Hier voeren we dan het ip-address van onze ‘target’ in.



Daarna kunnen we ‘Attacks’ zoeken die kunnen worden uitgevoerdt op onze host. Dit doen we door op ‘Attacks’ te klikken en dan op ‘Find attacks’.



Nu kunnen we met rechter muisknop op onze host ‘Attacks’ selecteren en uitvoeren. Wanneer een ‘attack’ gelukt is opent er meestal een nieuwe shell en krijgen we dit te zien.



### Windows OS

### Metasploitable OS

Op de Metasploitable OS hebben we veel ‘attacks’ uitgevoerd. We hebben eerst bij elke categorie een check gedaan welke exploits zouden kunnen werken. Daarna hebben we deze uitgeprobeerd. Uiteraard hebben we niet alles kunnen uitproberen maar dit was ons resultaat.

|  |  |  |
| --- | --- | --- |
| Categorie | Exploitable | Exploit |
| FTP | Exploitable | vsftpd\_234\_backdoor |
| Http | Not Exploitable (niet alles geprobeerd) |  |
| IRC | Exploitable | unreal\_ircd\_3281\_backdoor |
| Misc | Exploitable | java\_rmi\_server |
| Postgress | Not exploitable |  |
| Realserver | Not exploitable (Niet aanwezig) |  |
| Samba | Exploitable | usermap\_script |
| Smtp | Not exploitable |  |
| Ssh | Not exploitable |  |
| Telnet | Not exploitable |  |
| Vnc | Not exploitable |  |
| Webapp | Not exploitable (niet aanwezig) |  |
| Wyse | Not exploitable |  |
| X11 | Not exploitable (niet aanwezig) |  |

### Conclusie

Armitage is gemakkelijk en zeer krachtig. Op enkele minuten tijd zat je binnen in het systeem. Uiteraard was Metasploitable OS een gemakkelijk target maar toch waren we verbaasd over hoe snel en gemakkelijk het wel niet was om binnen te geraken.