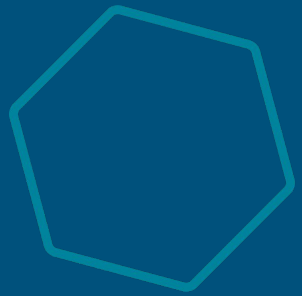


nessus®
Professional

Logiciel Nessus

Par Fensie Tibaut | 11 août 2022

Nessus ? Késako ?

c’est un scanner de sécurité réseau

Il détecte :

- les services vulnérables
- les fautes de configuration
- les patchs de sécurité non appliqués
- les mots de passe par défaut ou commun
- les services jugés faibles
- les possibles DDoS

Comment fait-il ça ?

- en identifiant un numéro de version
- en récupérant la liste des logiciels ou paquets installés

Comment fonctionne-t-il ?

- Basé sur une architecture client/serveur
- Compatible Windows et Linux
- Stocke et gère ses failles de sécurité avec des plugins (en C ou en NASL)

Comment fonctionne-t-il ?

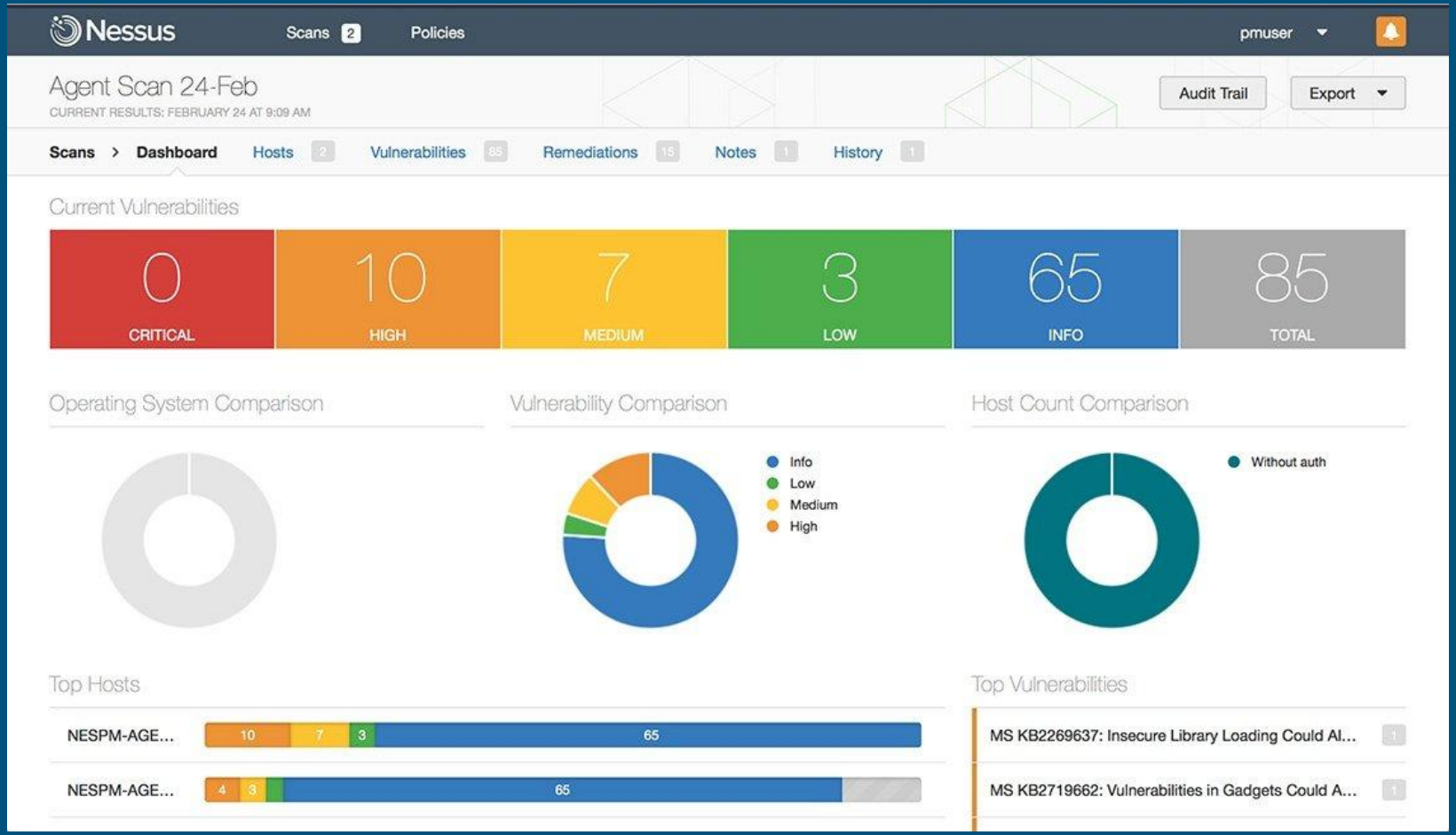
Il est divisé en 2 parties :

1. Nessusd : la partie serveur qui contient :
    1. nessus-update-plugins
    2. nessus-adduser
    3. nessus-mkcert

Il possède un fichier de configuration propre

2. Nessus : la partie client sert à :
    1. Se connecter au serveur
    2. envoyer la liste des machines à scanner

Il possède des exécutables pour la génération de rapports

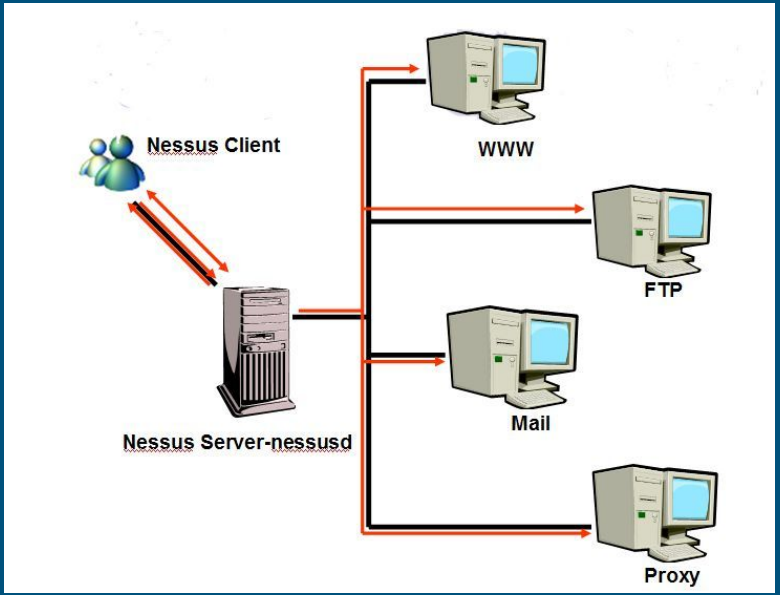


Visuel de l'interface

Comment fonctionne-t-il ?

Processus de fonctionnement :

1. Détecte si la machine est vivante
2. Scan des ports de la machine
3. Scan local ou distant
4. Récupération des données
5. Attaques de la machine de façon graduelle
    a. attaques simples
    b. attaques susceptibles d'être destructrices
    c. DDoS de logiciels
    d. DDoS de services



Le scan distant

Ressemble à nmap, il détermine :

- les ports ouverts
- le type des services utilisés

Avantages :

- plusieurs instances client
- plusieurs instances serveur
- plusieurs attaques simultanées sur une même cible
- attaques simultanées de différentes cibles

le soucis c'est de trouver le bon compromis Nbr hôte/bande passante

Inconvénients :

- Peut générer des faux positifs
- peut générer une surcharge du réseau

Le scan local

Pour ce type de scan Nessus a besoin :

- de se connecter en local sur la machine
- d'utiliser un compte local avec les accès les plus élevé (*root* ou *system*)

Avantages :

- plus complet que le scan distant
  - tests :
    - des mots de passe
    - des fautes de configurations de logiciels
    - des versions dll ou de packages obsolètes
    - des services désactivés ou vulnérables
- très rapide comme scan

Inconvénients :

- tests plus agressifs
- Détection par des IDS de Nessus comme une attaque de hacker

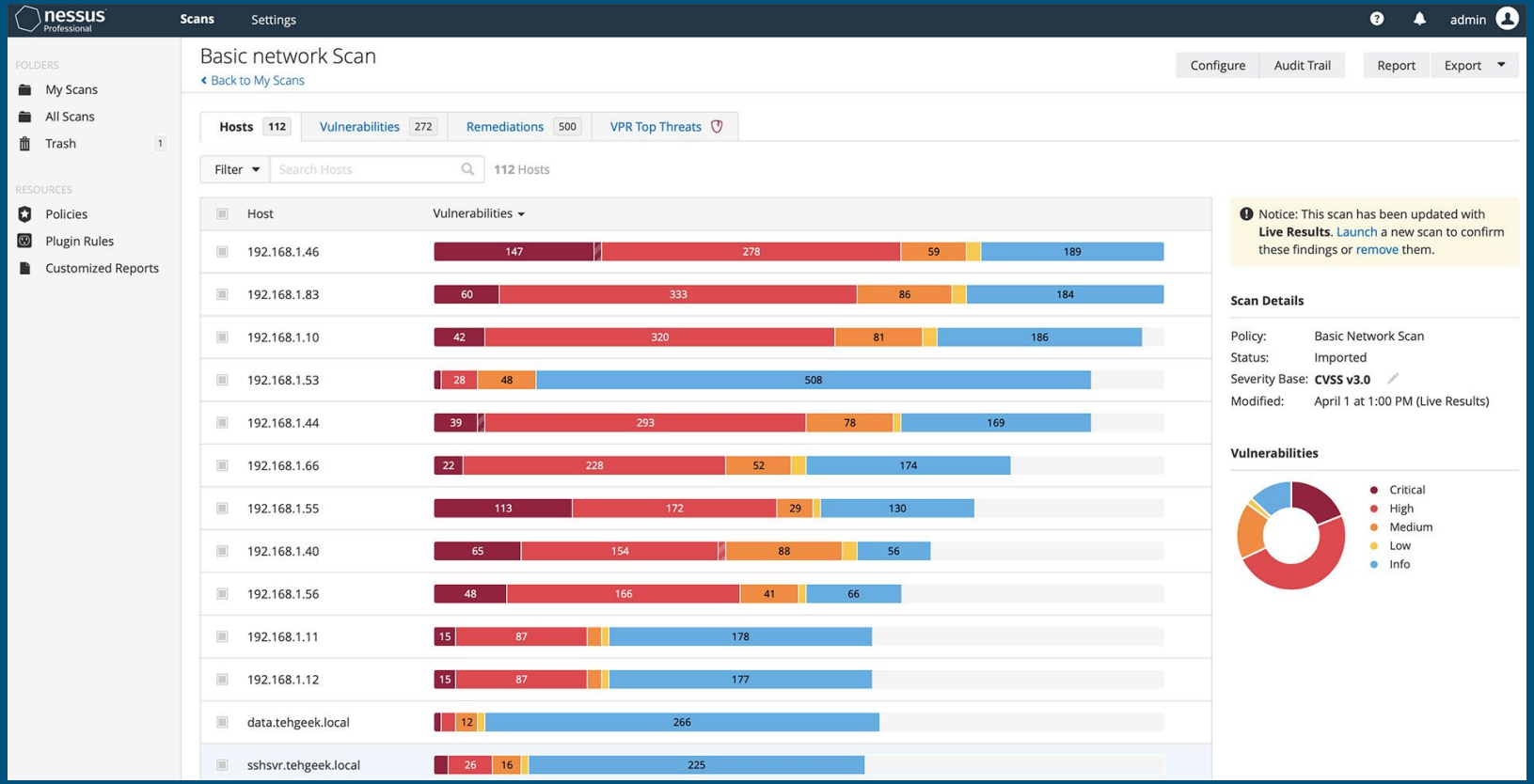
La gestion des rapports

un rapport contient :

- la liste des machines scannées
  - leurs OS
  - leurs services
    - la version
  - leurs vulnérabilités
    - une criticité
    - une description
    - une solution

ces rapports peuvent être exportés sous différents format :

- HTML simple ou avec graph
- XML
- LaTEX
- NSR
- NBE
- TXT



Rapport présenté dans l'interface

```
timestamps|||scan_start|Wed Oct 21 18:05:26 2009|
timestamps||192.168.0.2|host_start|Wed Oct 21 18:05:31 2009|
results|192.168.0|192.168.0.2|general/tcp|10180|Security Note|The remote host is up\n
results|192.168.0|192.168.0.2|general/icmp|10114|
        Security Warning|\nThe remote host answers to an ICMP timestamp request.
        This allows an attacker \nto know the date which is set on your machine.
        \n\nThis may help him to defeat all your time based authentication protocols.
        \n\nSolution : filter out the ICMP timestamp requests (13), and the outgoing ICMP
        \ntimestamp replies (14).\n\nRisk factor : Low\nCVE : CAN-1999-0524\n
results|192.168.0|192.168.0.2|general/udp|10287|Security Note|
        For your information, here is the traceroute to 192.168.0.2 :
        \n192.168.0.11
        \n192.168.0.2\n\n
results|192.168.0|192.168.0.2|general/tcp|19506|
        Security Note|Information about this scan :
        \n\nNessus version : 2.2.10\nPlugin feed version : 200704181215
        \nType of plugin feed : GPL only\nScanner IP : 192.168.0.11
        \nPort scanner(s) : synscan nessus_tcp_scanner
        \nPort range : 1-15000\nThorough tests : no
        \nExperimental tests : no
        \nParanoia level : 1
        \nReport Verbosity : 1
        \nSafe checks : yes
        \nMax hosts : 20
        \nMax checks : 4
        \nScan duration : unknown (ping_host.nasl not launched?)\n\n
results|192.168.0|192.168.0.2|general/tcp|9999|
        Security Hole|\nYou are running a version of Nessus which is not configured to receive
        \na full plugin feed. As a result, the security audit of the re
        \nincomplete results.
        \n\nTo obtain a complete plugin feed, you need to register your
        \nat http://www.nessus.org/register/ then run nessus-update-plu
        \nthe full list of Nessus plugins.\n\n
timestamps||192.168.0.2|host_end|Wed Oct 21 18:07:53 2009|
timestamps|||scan_end|Wed Oct 21 18:07:53 2009|
```


```
timestamps|||scan_start|Wed Oct 21 18:05:26 2009|
timestamps||192.168.0.2|host_start|Wed Oct 21 18:05:31 2009|
results|192.168.0|192.168.0.2|general/tcp|10180|Security Note|The remote host is up\n
results|192.168.0|192.168.0.2|general/icmp|10114|Security Warning|\nThe remote host ans
results|192.168.0|192.168.0.2|general/udp|10287|Security Note|For your information, her
results|192.168.0|192.168.0.2|general/tcp|19506|Security Note|Information about this sc
results|192.168.0|192.168.0.2|general/tcp|9999|Security Hole|\nYou are running a versio
timestamps||192.168.0.2|host_end|Wed Oct 21 18:07:53 2009|
timestamps|||scan_end|Wed Oct 21 18:07:53 2009|
```


Exemple de rapport en .NBE

La sécurité dans Nessus

1. sécurité physique du serveur
2. sécurité logique du serveur
3. Configuration des droits du serveur
4. Configuration du serveur pour les scans locaux

```
SNMP settings[entry]:SNMPv3 user name : =
SNMP settings[password]:SNMPv3 authentication password : =
SNMP settings[password]:SNMPv3 privacy password : =
# Pour telnet, rsh, rexec :
Cleartext protocols settings[entry]:User name : =
Cleartext protocols settings[password]:Password (unsafe!) : =
SSH settings[entry]:SSH user name : = root
SSH settings[radio]:Elevate privileges with : = Nothing;sudo;su
SSH settings[entry]:Preferred SSH port : = 22
SSH settings[password]:SSH password (unsafe!) : =
SSH settings[file]:SSH public key to use : =
SSH settings[file]:SSH private key to use : =
SSH settings[password]:Passphrase for SSH key : =
SSH settings[password]:su/sudo password : =
SSH settings[file]:SSH known_hosts file : =
SSH settings[entry]:Client version : = OpenSSH_5.0
Kerberos configuration[entry]:Kerberos Key Distribution Center (KDC) : =
Kerberos configuration[entry]:Kerberos Realm (SSH only) : =
Services[file]:SSL certificate : =
Services[file]:SSL private key : =
Services[password]:PEM password : =
Services[file]:CA file : =
Database settings[entry]:Login : =
Database settings[password]:Password : =
Database settings[entry]:Database SID : =
Database settings[entry]:Database port to use : =
Login configurations[entry]:HTTP account : =
Login configurations[password]:HTTP password (sent in clear) : =
Login configurations[entry]:NNTP account : =
Login configurations[password]:NNTP password (sent in clear) : =
Login configurations[entry]:POP2 account : =
Login configurations[password]:POP2 password (sent in clear) : =
Login configurations[entry]:POP3 account : =
Login configurations[password]:POP3 password (sent in clear) : =
Login configurations[entry]:IMAP account : =
Login configurations[password]:IMAP password (sent in clear) : =
Login configurations[entry]:SMB account : = admin
Login configurations[password]:SMB password : = password
Login configurations[entry]:SMB domain (optional) : =
Login configurations[entry]:SNMP community (sent in clear) : =
SLAD Init[file]:slad SSH public key: =
SLAD Init[file]:slad SSH private key: =
SLAD Init[password]:slad SSH key passphrase: =
Global variable settings[checkbox]:Do not log in with user accounts not specified in the policy = no
Global variable settings[file]:SSL certificate to use : =
Global variable settings[file]:SSL CA to trust : =
Global variable settings[file]:SSL key to use : =
Global variable settings[password]:SSL password for SSL key : =
```

Conclusion


Merci pour votre attention