Quantalytics

Q-Vul®

L'appliance réseau **Q-Vul**® est un appliance de réseau de test de vulnérabilité et de reporting créée à l'aide d'**OpenVAS** («Open Vulnerability Assessment System»). **OpenVAS**, précédemment appelé GNessUs, a commencé comme une fourchette de l'outil de recherche de vulnérabilité de **Nessus**® après que Tenable Security a retiré sa version open source **Nessus** en 2004. **OpenVAS** a évolué depuis lors à la fois par rapport à son moteur de balayage et les vulnérabilités qu'il peut trouver et identifier. Actuellement, il peut trouver et identifier plus de 47,000 vulnérabilités de sécurité dans une variété de systèmes d'exploitation, y compris Windows, IOS et Linux. Il peut également identifier les vulnérabilités dans divers appareils réseau, y compris les routeurs, les commutateurs intelligents et les périphériques IoT.

L'utilisation se fait via une interface Web

L'appliance réseau **Q-VUL** met automatiquement à jour les tests de vulnérabilité de réseau (NVT) d'**OpenVAS** à l'aide de l'alimentation **OpenVAS** NVT. **L'OpenVAS** NVT Feed est mis à jour au moins une fois par semaine lorsque de nouvelles vulnérabilités sont trouvées. En plus d'utiliser le flux public NVT, les utilisateurs peuvent ajouter des NVT privés.

L'appliance réseau **Q-VUL** est destinée à être placée sur un réseau et à exécuter des analyses soit après la publication de nouvelles NVT, soit lors de l'introduction de nouveaux matériels ou logiciels. Les analyses peuvent être programmées aussi souvent que vous le souhaitez. Nous recommandons des balayages nocturnes automatisés en plus de la numérisation après les mises à jour NVT.

Spécifications matérielles Q-VUL :

- 108 mm x 64 mm x 26 mm – 170 grammes (4.25" x 2.50" x 1.125" – 6 oz)
- Consommation électrique à pleine charge: 8 watts, 120v-240v
- Pas de ventilateur ou de pièces mobiles. Doit être installé dans un espace bien ventilé.
- Fonctionne de 0°C à 70°C (32°F–158°F)

Indicateurs LED:

- Pouvoir électrique
- Lien (connexion physique au réseau)
- Activité (trafic réseau)
- 1000 mbps (gigabit) NIC connexion
- WiFi Bi-Bande. (2.4 GHz et 5 GHz)

Le système de réseau **Q-Vul** comprend:

- **OpenVAS** – **OpenVAS** est le principal groupe de test et de déclaration de vulnérabilité de classe entreprise open source pour les logiciels et le matériel, y compris les périphériques IoT. **OpenVAS** inclut la mise à jour automatique des tests de vulnérabilité réseau (NVT) ainsi que la possibilité de planifier des analyses. **OpenVAS** comprend également des rapports complets.
- **Webmin - Webmin** est utilisé pour l'entretien ménager des réseaux et la configuration du réseau.

Contact: Richard Avery
+1 646-449-7810
Q-Vul@quantalytics.com

Quantalytics. Défenses de réseau en profondeur.

- **HA Proxy – HA Proxy** est le premier fournisseur open source pour le basculement automatique et l'équilibrage de charge. Jusqu'à 32 appareils de réseau **Q-Vul** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement grands. L'administration se fait via un web gui.
- **ModSecurity® – ModSecurity®** («**ModSec**») est le premier package de protection contre les attaques du serveur Web Apache. **ModSec** est utilisé pour endurer le serveur web Apache intégré de l'appliance **Q-Vul** et éviter les attaques imaginables.
- **Tiny Honeypot («THP») - THP** trompe les attaquants en faisant apparaître que l'attaque fonctionne, tout en enregistrant les informations d'attaque. **THP** gaspille le temps d'un attaquant et crée l'opportunité de détecter l'intrusion du réseau en offrant à l'attaquant ce qui semble être des milliers de services.
- **ClamAV®** – **ClamAv®** est le premier package antivirus open source.

L'appliance de réseau **Q-Vul** possède possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Bi-Bande 802.11 (2.4 GHz & 5 GHz). L'appliance réseau **Q-Vul** est également disponible en tant que Machine Virtuelle («VM»).

L'appliance réseau **Q-Vul** est complètement administrée via une interface graphique Web. Aucune interface de ligne de commande («CLI») ou Linux n'est requise.

En utilisant le module **Webmin** fourni, l'authentification à deux facteurs peut être ajoutée à l'aide de **Google Authenticator** ou **Authy**, un service commercial avec sa propre application. **Google Authenticator** s'exécute sur les appareils Android, IOS et Blackberry, et utilise le protocole standard de TOTP.

Les notifications sont fournies par e-mail à l'aide de **SendMail**, qui est configuré avec un module dans **Webmin** et les entrées syslog. L'appliance de réseau **Q-Vul** peut être intégré à **Nagios®** sur le **Q-Box®** comme autre voie de notification. La notification par SMS est disponible en option. L'appliance de réseau **Q-Vul** peut également être intégré au **Q-Log®** ou à toute autre solution syslog ou SIEM. (Security Information and Event Management).

Contact: Richard Avery
+1 646-449-7810
Q-Vul@quantalytics.com