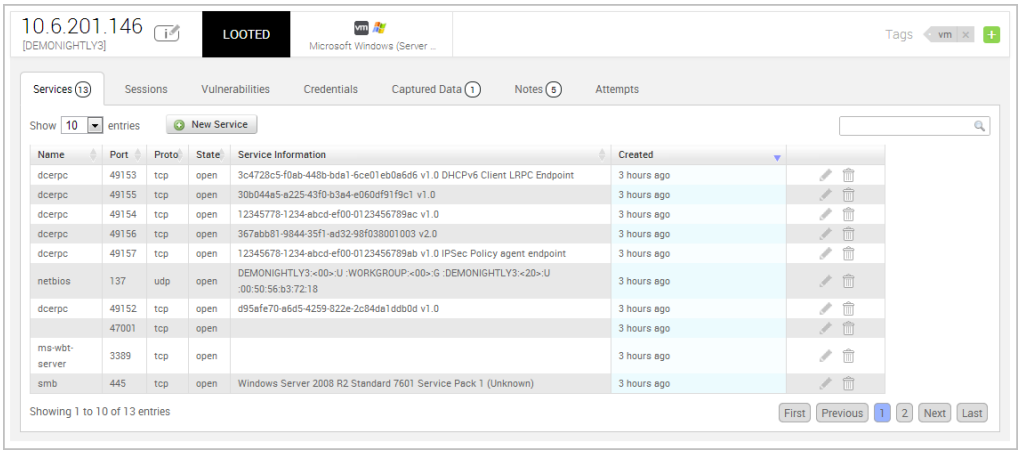
Metasploit Pro Edition

Mettez votre défense à l'épreuve, de manière plus efficace, avec Metasploit

L'anticipation des actions de vos adversaires vous permet de mieux préparer votre défense. Appuyé par une communauté open source composée de 200 000 membres, Metasploit est en mesure de vous fournir ces informations. Il s'agit de la solution de test d'intrusion la plus réputée dans le monde. Avec une moyenne de 1,2 exploit ajouté chaque jour, Metasploit vous permet de localiser votre point faible avant qu'une personne malveillante ne le fasse.

Exécutez des tests d'intrusion 45 % plus rapidement

De nombreux tests d'intrusion impliquent des démarches exigeant beaucoup de temps, faisant ainsi perdre un temps précieux aux experts avertis en sécurité. Par conséquent, les évaluations de la sécurité se limitent aux contrôles ponctuels amenant ainsi les organisations à percevoir de manière erronée leur posture sécuritaire, dû à leur portée limitée. La formation de nouveaux professionnels est difficile et coûteuse.



Metasploit Pro aide les testeurs d'intrusion à exécuter les évaluations de manière plus efficace en accélérant les tâches courantes, telles que la découverte, l'exploitation et la rédaction de rapport, en proposant des méthodes d'évasion et de post exploitation ainsi qu'en gérant de manière efficace la quantité considérable de données générées lors des évaluations à grande échelle.

Les professionnels de la sécurité souhaitant s'initier aux tests d'intrusion réaliseront le potentiel de productivité présenté par Metasploit Pro comparé aux autres solutions open source.

Achevez les tâches 45 % plus rapidement grâce à une productivité accrue : les testeurs d'intrusion se doivent d'utiliser leur précieuse expertise de manière efficace. Sur une étude composée de plus de 2 000 utilisateurs Metasploit, les utilisateurs Metasploit Pro affirment que le programme leur fait gagner du temps, 45 % en moyenne, par rapport à Metasploit Framework.

Tirez parti du projet open source Metasploit ainsi que de sa bibliothèque d'exploits, première sur le marché : appuyé par une communauté composée de plus de 200 000 membres, Rapid7 est en charge de la gestion du projet Metasploit, la plus grande collection d'exploits passés en revue. Ceci permet à Rapid7 d'obtenir des informations uniques sur les dernières méthodes et approches des personnes malveillantes.

Gérez les données lors des évaluations à grande échelle : l'exécution d'une évaluation de réseaux sur une centaine d'hébergeurs peut se présenter comme un défi. Metasploit Pro s'adapte afin de pouvoir prendre en charge des milliers d'hébergeurs.

Contournez les solutions de défense : créez des données utiles et dynamiques permettant de contourner la détection par des solutions contre les logiciels malveillants. Metasploit Pro contourne les solutions antivirus 90 % du temps ; il est à noter qu'aucune solution n'est en mesure de détecter l'intégralité des options. Contournez le pare-feu ainsi que le scanneur de prévention d'intrusions grâce à des techniques d'évasion au niveau du trafic.

Prenez le contrôle des ordinateurs compromis et du réseau : choisissez parmi plus de 200 modules de post exploitation, allant de la copie de fichiers à l'installation d'enregistreurs de frappe. Les macros de post exploitation peuvent automatiser l'exécution de vos étapes privilégiées lorsqu'un nouvel ordinateur est compromis. Une fois que vous avez atteint le premier ordinateur, vous serez en mesure de contrôler l'intégralité du réseau, particulièrement lorsque vous avez recours à la création de relais au sein du RPV pour obtenir un accès complet au réseau local.

Générez automatiquement des rapports contenant les principaux résultats : la rédaction de rapport représente, la plupart du temps, le côté frustrant de la tâche et peut prendre jusqu'à 30 % du temps réservé à une évaluation. Générez des rapports pour afficher vos résultats et procédez à un triage par réglementation, telle que PCI DSS et FISMA.

Avantages principaux

Test d'intrusion

- Achevez les tâches 45 % plus rapidement grâce à une productivité accrue
- Tirez parti du projet open source Metasploit ainsi que de sa bibliothèque d'exploits, première sur le marché
- Gérez les données lors des évaluations à grande échelle
- Contournez les solutions de défense
- Prenez le contrôle des ordinateurs compromis et du réseau
- Générez automatiquement des rapports contenant les principaux résultats

Validation de la vulnérabilité

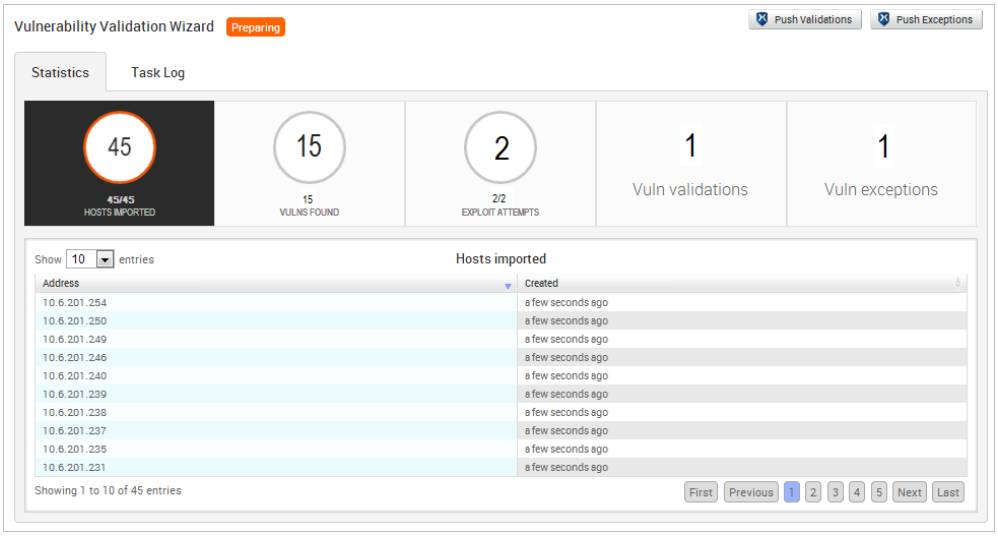
- Créez des rapports de correction en boucle fermée et hiérarchisés
- Améliorez la sécurité en privilégiant les vulnérabilités exploitables
- Prouvez l'efficacité de la correction ou du contrôle compensatoire auprès des auditeurs

Gestion de la sensibilisation à l'hameçonnage

- Accédez à une visibilité complète des risques courus par les utilisateurs en intégrant UserInsight de Rapid7
- Accédez à la sensibilisation globale des utilisateurs et offrez une formation ciblée
- Testez l'efficacité des contrôles de sécurité
- Lancez des campagnes de simulation à la sensibilisation à l'hameçonnage pour des milliers d'utilisateurs

Validez les vulnérabilités afin de hiérarchiser les vulnérabilités à des fins de correction

Les scanneurs de vulnérabilité peuvent détecter le logiciel installé ainsi que ses vulnérabilités ; cependant, ils ne permettent pas de déterminer s'il représente un risque élevé pour votre réseau. Ceci peut représenter un danger potentiel, car les équipes informatiques ne sont pas en mesure de déterminer les vulnérabilités à traiter en priorité.

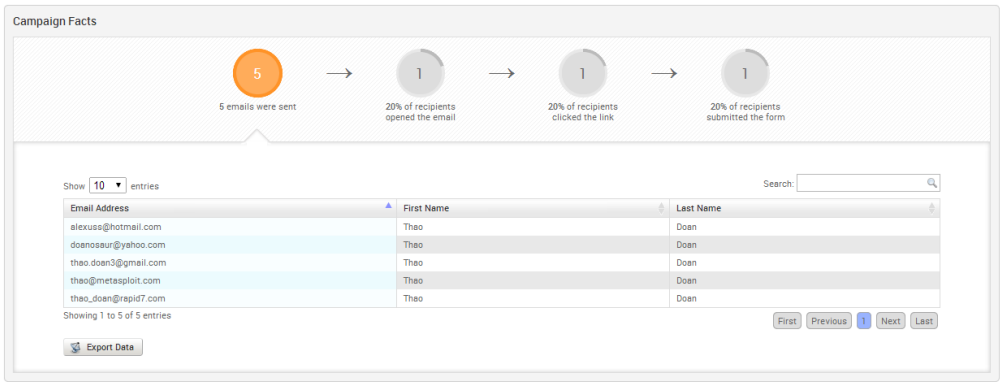


La validation de vulnérabilité teste l'exploitabilité des vulnérabilités afin de démontrer le risque de manière objective, évitant ainsi les discussions concernant le niveau de risque d'une vulnérabilité.

Metasploit Pro termine le processus de validation de vulnérabilité par l'envoi des résultats à Nexpose, où l'exploitabilité d'une vulnérabilité peut être utilisée pour créer des rapports et hiérarchiser les vulnérabilités à des fins de correction.

Gérez la sensibilisation à l'hameçonnage afin de réduire les risques courus par l'utilisateur

La plupart du temps, les utilisateurs représentent le maillon faible de la chaîne de sécurité, en exposant les organisations aux attaques. L'hameçonnage a particulièrement connu une hausse au cours des dernières années. De nombreuses organisations proposent éventuellement des formations aux utilisateurs finaux. Toutefois, il leur est difficile d'identifier les utilisateurs qui risquent encore de tomber dans le piège des courriers électroniques d'hameçonnage et d'exposer ainsi l'organisation à des risques divers.



Metasploit Pro de Rapid7 mesure l'efficacité des formations de sensibilisation à la sécurité en exécutant des campagnes de simulation d'hameçonnage, ce qui permet d'aider à gérer l'exposition à ce vecteur d'attaque courant.

Metasploit Pro intègre UserInsight de Rapid7 afin d'ajouter les risques d'hameçonnage dans le cadre des risques courus par l'utilisateur. Cette intégration comprend l'accès réseau, l'utilisation du service en nuage ainsi que les identifiants compromis.

Témoignages de nos clients

« La gestion du temps est essentielle et Metasploit Pro aide beaucoup dans ce domaine. Nous utilisons Metasploit Pro en grande partie, car il nous fait gagner du temps [...]
Nos clients devraient constamment avoir recours à Metasploit Pro au lieu de leur système réseau habituel. Si nous détectons des problèmes sur un réseau en exécutant un balayage standard de Metasploit, c'est que ce client a de sérieux problème ».

- *Jim O'Gorman, président d' Offensive Security*

« Après huit mois d'utilisation de Nexpose et de Metasploit, nous avons procédé à un audit de conformité. Comparé à l'année précédente, nous avons été en mesure de réduire les risques d'exposition de plus de 98 %. Ceci est particulièrement impressionnant en considérant le fait que nous avons fait l'acquisition de cinq nouveaux hôpitaux au cours de cette période ; ceci démontre que l'utilisation de Metasploit avant une acquisition fait une différence considérable. Notre objectif actuel est d'utiliser Metasploit sur l'intégralité de nos actifs chaque trimestre ».

- *Scott Erven, chargé de la sécurité des informations à Essentia Health*

À propos de Rapid7

Les solutions d'analyse de Rapid7 recueillent, contextualisent et analysent les données liées à la sécurité dont vous avez besoin pour lutter contre un adversaire de plus en plus répandu et trompeur. Contrairement aux évaluations de la vulnérabilité ou aux gestions des incidents traditionnelles, les solutions Rapid7 donnent un aperçu exclusif de l'état de vos actifs et de vos utilisateurs sur des réseaux en nuage virtuels, mobiles, privés et publics. Elles vous permettent de gérer entièrement vos risques, de simplifier la conformité et d'identifier, enquêter et arrêter les menaces plus rapidement. Nos services de renseignements spécialisés dans les menaces informatiques, notre communauté open source Metasploit et les laboratoires Rapid7, leaders du secteur, fournissent un contexte pertinent, des mises à jour en temps réel et une hiérarchie des risques. Nos solutions sont utilisées par plus de 25 % des entreprises du classement Fortune 1 000 et environ 3 000 entreprises et organisations gouvernementales dans 78 pays. Pour en savoir plus sur Rapid7 ou participer à notre recherche sur les menaces, consultez la page www.rapid7.com.

Rapid 7 EMEA Headquarters 1st Floor, Building 1025, Arlington House, Arlington Business Park, Reading, RG74SA, UK +44 (0) 1183 703 500 www.rapid7.com