Rapport Global

rapport_connexion_20240621_091026.docx

rapport_scan_192.168.100.15_20240621_090136.docx

Adresse cible: 192.168.100.15

rapport_scan_cve_20240621_093602_00e08168-3379-4a70-9f88-8bc7d904cbcd.docx

Rapport de Connexion (Temp)

Tests de Connexion IP

8.8.8.8 (DNS Public Google) : OK

8.26.56.26 (DNS Sécurisé Comodo) : OK

208.67.222.222 (OpenDNS) : OK

1.0.0.1 (DNS Cloudflare (Alternatif)) : OK

64.6.65.6 (Neustar DNS (Alternatif)) : OK

198.41.0.4 (DNS Public Verisign) : OK

8.20.247.20 (DNS Sécurisé Comodo (Alternatif)) : OK

9.9.9.9 (DNS Quad9) : OK

4.2.2.3 (DNS Level3 (Alternatif)) : OK

4.2.2.5 (DNS Level3 (Alternatif)) : OK

1.1.1.1 (DNS Cloudflare) : OK

195.46.39.39 (SafeDNS) : OK

45.90.28.0 (NextDNS) : OK

4.2.2.2 (DNS Level3 (Alternatif)) : OK

4.2.2.6 (DNS Level3 (Alternatif)) : OK

77.88.8.8 (DNS Yandex) : OK

4.2.2.1 (DNS Level3) : OK

64.6.64.6 (Neustar DNS) : OK

208.67.220.220 (OpenDNS (Alternatif)) : OK

199.7.83.42 (UltraDNS) : OK

Tests de Connexion Domaines

dropbox.com : OK (tentatives: 1)

wordpress.com : OK (tentatives: 1)

linkedin.com : OK (tentatives: 1)

netflix.com : NON (tentatives: 3)

tumblr.com : OK (tentatives: 1)

apple.com : OK (tentatives: 1)

microsoft.com : OK (tentatives: 1)

impots.gouv.fr : NON (tentatives: 3)

ebay.com : OK (tentatives: 1)

pinterest.com : OK (tentatives: 1)

twitter.com : OK (tentatives: 1)

live.com : OK (tentatives: 1)

whatsapp.com : OK (tentatives: 1)

snapchat.com : OK (tentatives: 1)

amazon.com : OK (tentatives: 1)

github.com : OK (tentatives: 1)

yahoo.com : OK (tentatives: 1)

paypal.com : OK (tentatives: 1)

reddit.com : OK (tentatives: 1)

palamini.fr : NON (tentatives: 3)

Test de Débit

Liaison descendante : 347.27 Mb/s

Liaison montante : 107.08 Mb/s

Rapport de scan pour 192.168.100.15

Généré le : 21-06-2024 09:01:36

Scan des ports:

Port 135 (Service inconnu): open

Port 137 (NetBIOS Name Service): filtered

Port 139 (NetBIOS Session Service): open

Port 445 (Microsoft-DS Active Directory, partages Windows): open

Port 902 (Service inconnu): open

Port 912 (Service inconnu): open

Supposition du système d'exploitation:

Microsoft Windows 10 1809 - 2004 (Précision: 100%)

Services détectés:

Port 135: msrpc

Port 139: netbios-ssn

Port 445: microsoft-ds

Port 902: vmware-auth

Port 912: vmware-auth

Port 3389: ms-wbt-server

Bannières collectées:

Port 135: Microsoft Windows RPC

Port 139: Microsoft Windows netbios-ssn

Port 445:

Port 902: VMware Authentication Daemon

Port 912: VMware Authentication Daemon

Port 3389: Microsoft Terminal Services

Rapport de Scan CVE

Services

Service: msrpc, Version:

Description: Le service msrpc (Microsoft Remote Procedure Call) est un protocole de communication réseau utilisé par les systèmes Microsoft pour permettre à des programmes de s'exécuter sur des machines distantes et d'échanger des données. Il facilite la communication entre différents processus sur un réseau local ou distant.

Service: netbios-ssn, Version:

Description: Le service NetBIOS-SSN (NetBIOS Session Service) est utilisé pour gérer des sessions de communication entre différents systèmes sur un réseau utilisant le protocole NetBIOS. Il permet l'établissement, la maintenance et la fin de sessions de communication entre les ordinateurs, facilitant ainsi l'échange de données et de services. Ce service peut être utilisé pour des partages de fichiers, des impressions réseau, ou d'autres applications nécessitant une communication entre des machines sur un réseau local.

Service: microsoft-ds, Version:

Description: Le service Microsoft-DS est un service de partage de fichiers utilisé par les systèmes d'exploitation Windows. Il permet d'accéder aux fichiers et aux ressources partagés sur un réseau local.

Service: vmware-auth, Version: 1.10

Description: Le service vmware-auth est un service d'authentification de VMware, utilisé pour vérifier l'identité des utilisateurs et leur accès aux ressources et services du réseau VMware. Il permet de contrôler et de sécuriser l'accès aux machines virtuelles et aux autres ressources de l'environnement virtualisé.

Service: vmware-auth, Version: 1.0

Description: Le service vmware-auth est un composant de VMware qui gère l'authentification des utilisateurs se connectant aux solutions VMware, telles que vSphere et VMware NSX. Il permet de vérifier l'identité des utilisateurs et de contrôler leur accès aux ressources du système.

Service: ms-wbt-server, Version:

Description: Le service ms-wbt-server est un service Windows qui permet aux utilisateurs de se connecter à distance à un ordinateur via le protocole de bureau à distance (ou Remote Desktop). Il permet ainsi le contrôle à distance de l'ordinateur, généralement utilisé pour l'assistance technique ou l'administration à distance.

Service: tcpwrapped, Version:

Description: Le service TCPwrapped est un mécanisme de sécurité qui protège un serveur en restreignant l'accès aux applications réseau qui tournent sur une machine. Il sert à limiter les connexions entrantes non autorisées en enveloppant les services réseau sous un wrapper de sécurité.

Vulnérabilités

Service: msrpc (Version:)

CVE ID: CVE-2002-1873
Description: CVE-2002-1873 est une vulnérabilité de type déni de service affectant les systèmes Unix, y compris Linux. Un attaquant distant peut exploiter cette faille en envoyant des paquets UDP malveillants, provoquant un plantage du système ou entraînant la saturation de la mémoire.
Recommandation: La vulnérabilité CVE-2002-1873 concerne une faille d'authentification dans certains systèmes. Pour la mitiger, vérifiez et mettez à jour les configurations d'authentification, limitez l'accès aux ressources sensibles et surveillez les tentatives d'accès non autorisées. Assurez-vous également de sensibiliser les utilisateurs à l'importance de la sécurité des identifiants et mots de passe.

CVE ID: CVE-2018-8407
Description: Le CVE-2018-8407 est une vulnérabilité de type exécution de code à distance dans Microsoft Internet Explorer. Cette faille affecte les systèmes Windows et peut permettre à un attaquant d'exécuter du code malveillant à distance. L'impact potentiel est la

prise de contrôle complète du système ciblé par l'attaquant.
Recommandation: La vulnérabilité CVE-2018-8407 est liée à une exposition d'informations sensibles dans Azure DevOps Server. Pour mitiger cette vulnérabilité, assurez-vous de mettre à jour vers la dernière version du logiciel, suivez les bonnes pratiques de sécurité et limitez l'accès aux données sensibles.

Service: microsoft-ds (Version:)

CVE ID: CVE-2024-35927
Description: Le CVE-2024-35927 est une vulnérabilité de type dépassement de tampon affectant les systèmes utilisant le protocole TCP/IP. L'exploitation de cette vulnérabilité pourrait permettre à un attaquant distant d'exécuter du code arbitraire ou de provoquer un déni de service. Il est recommandé de mettre en place des correctifs ou des mesures de protection pour atténuer les risques associés.
Recommandation: La vulnérabilité CVE-2024-35927 concerne une faille de sécurité dans le protocole TLS. Pour mitiger cette vulnérabilité, assurez-vous de mettre à jour vos systèmes pour appliquer les correctifs disponibles, surveillez activement les tentatives d'exploitation et limitez l'exposition en restreignant l'accès aux services concernés.

CVE ID: CVE-2024-35931
Description: Le CVE-2024-35931 est une vulnérabilité de type exécution de code à distance qui affecte les systèmes d'exploitation Windows Server. Un attaquant pourrait exploiter cette faille pour exécuter du code malveillant à distance, compromettant ainsi la sécurité du système.
Recommandation: La recommandation pour le CVE-2024-35931 est de mettre à jour immédiatement le logiciel concerné pour appliquer le correctif de sécurité fourni par l'éditeur. Assurez-vous également de restreindre l'accès aux ports vulnérables pour limiter l'exposition à d'éventuelles attaques. Effectuez régulièrement des audits de sécurité pour détecter toute activité suspecte ou tentative d'exploitation de la vulnérabilité.

CVE ID: CVE-2002-0597
Description: Le CVE-2002-0597 est une vulnérabilité de type débordement de tampon dans le serveur FTP ProFTPD (Clame acclamé ProFTPD, le serveur ProFTPD est utilisé pour fournir des services FTP sécurisés.) version 1.2.5 et inférieure, cette vulnérabilité permet à un attaquant distant d'exécuter du code arbitraire ou de provoquer un déni de service.
Recommandation: La vulnérabilité CVE-2002-0597 concerne une faille dans le service RPC Portmapper. Pour mitiger cette vulnérabilité, il est recommandé de restreindre l'accès au service Portmapper aux machines nécessaires via un pare-feu, de maintenir à jour les correctifs de sécurité sur les systèmes affectés, et de surveiller activement les activités réseau pour détecter toute tentative d'exploitation.