1. Quelle commande est utilisée pour activer SMB 1.0 sur un serveur Windows ?

A. Set-SmbServerConfiguration –EnableSMB1Protocol $true

B. Enable-SmbServer -Version SMB1.0

C. Enable-SmbProtocol -SMB 1.0

D. Start-SMB1 -Server

2. Quelle est la commande dans PowerShell pour désactiver SMB 1.0 et activer SMB 3.1.1 avec chiffrement ?

A. Set-SmbServer -DisableSMB1 -EnableSMB3 -EncryptData $true

B. Disable-Smb1 -EnableSMB2 -Encrypt $true

C. Set-SmbServerConfiguration –EnableSMB1Protocol $false –EnableSMB2Protocol $true –EncryptData $true

D. Set-SMBVersion -DisableSMB1 -EnableSMB3

3. Quelle commande permet de capturer les événements d'accès SMB audités dans Windows ?

A. Get-EventLog -LogName SMB/Audit

B. Get-WinEvent -LogName Microsoft-Windows-SMBServer/Audit

C. Audit-EventLog -SMBServer

D. Capture-Logs SMB/Audit

4. Quelle commande PowerShell permet de créer un partage SMB avec le chiffrement activé ?

A. New-SmbShare –Name "Partage" –Path "C:\Dossier" –EncryptData $true

B. Create-SmbShare –Name "Partage" –Encrypt $true

C. Set-SmbShare –Encrypt $true –Name "Partage"

D. Share-Dir –EncryptData $true –Path "C:\Dossier"

5. Comment désactiver SMB 1.x sur un serveur Windows 2016 ?

A. Set-SmbServerConfiguration –DisableSMB1 $false

B. Set-SmbServerConfiguration –EnableSMB1Protocol $false

C. Disable-SMB1Protocol –Force

D. Stop-SMB1 –Server 2016

6. Quelle option décrit correctement la différence entre le mode transport et le mode tunnel dans IPsec ?

A. Le mode transport chiffre uniquement la charge utile, tandis que le mode tunnel chiffre l'intégralité du paquet IP

B. Le mode tunnel chiffre uniquement l'en-tête IP, tandis que le mode transport chiffre tout le paquet

C. Le mode transport utilise un seul protocole, tandis que le mode tunnel utilise deux protocoles distincts

D. Le mode tunnel est plus rapide que le mode transport

7. Dans IPsec, quel protocole permet la négociation des clés et des paramètres de sécurité entre les deux parties ?

A. ESP (Encapsulating Security Payload)

B. AH (Authentication Header)

C. IKE (Internet Key Exchange)

D. TLS (Transport Layer Security)

8. Quel est l'objectif principal de l'AH (Authentication Header) dans IPsec ?

A. Assurer l'intégrité et l'authenticité des paquets sans les chiffrer

B. Chiffrer les paquets pour garantir leur confidentialité

C. Garantir la négociation des clés entre les pairs IPsec

D. Protéger l'en-tête IP uniquement

9. Quel protocole VPN est généralement considéré comme peu sécurisé en raison de vulnérabilités connues ?

A. OpenVPN

B. IKEv2/IPsec

C. PPTP

D. WireGuard

10. Quel protocole VPN utilise SSL/TLS pour le chiffrement et est particulièrement recommandé pour contourner les pare-feux stricts ?

A. OpenVPN

B. PPTP

C. L2TP/IPsec

D. SSTP

11. Quel protocole VPN est connu pour ses performances rapides sur les réseaux mobiles et sa capacité à reprendre les connexions automatiquement ?

A. L2TP/IPsec

B. IKEv2/IPsec

C. PPTP

D. OpenVPN

12. Quel protocole VPN est open source, moderne, et se distingue par sa simplicité de configuration et ses algorithmes de chiffrement avancés ?

A. SSTP

B. WireGuard

C. MPLS VPN

D. Cisco AnyConnect

13. Quel protocole VPN combine L2TP pour le tunneling et IPsec pour le chiffrement, offrant ainsi une sécurité renforcée mais une performance potentiellement réduite ?

A. IKEv2/IPsec

B. OpenVPN

C. PPTP

D. L2TP/IPsec

14. Quel est l'un des principaux avantages de SSTP par rapport aux autres protocoles VPN ?

A. Il est open source et multiplateforme

B. Il traverse facilement les pare-feux grâce à son utilisation du port 443 (HTTPS)

C. Il offre la meilleure performance sur les réseaux mobiles

D. Il est le plus sécurisé parmi les protocoles VPN

15. Quel protocole VPN utilise ChaCha20 pour le chiffrement et est optimisé pour des performances rapides et un faible encombrement de code ?

A. OpenVPN

B. WireGuard

C. L2TP/IPsec

D. Cisco AnyConnect

16. Quel protocole VPN est souvent utilisé dans les environnements d'entreprise avec une infrastructure réseau Cisco ?

A. OpenVPN

B. WireGuard

C. Cisco AnyConnect

D. PPTP

17. Quel protocole VPN est conçu pour être très léger, avec un code source minimaliste, facilitant les audits de sécurité ?

A. IKEv2/IPsec

B. WireGuard

C. OpenVPN

D. L2TP/IPsec

18. Quel protocole VPN est intégré de manière native dans les environnements Windows, permettant une utilisation transparente avec le système ?

A. PPTP

B. SSTP

C. WireGuard

D. OpenVPN

19. Quel mode d'IPsec est utilisé pour protéger uniquement le contenu des paquets IP, sans toucher aux en-têtes ?

A. Mode transport

B. Mode tunnel

C. Mode routage

D. Mode réseau

20. Quelle est la fonction principale du protocole ESP dans IPsec ?

A. Assurer l'intégrité des données uniquement

B. Assurer le chiffrement et l'intégrité des données

C. Gérer les clés de sécurité

D. Rediriger les paquets

21. Quel est le rôle principal de l'IKE (Internet Key Exchange) dans IPsec ?

A. Chiffrer les paquets de données

B. Authentifier les utilisateurs

C. Négocier les clés et les paramètres de sécurité

D. Gérer les tunnels VPN

22. Quelle technique IPsec est utilisée pour prévenir les attaques de rejeu (replay attacks) ?

A. AES-256

B. Compteurs de séquence

C. Table de hachage

D. Clé publique

23. Quelle commande permet de vérifier toutes les actions de filtrage IPSec configurées ?

A. `netsh ipsec static show filteraction`

B. `netsh ipsec static show policy all`

C. `netsh ipsec static delete filteraction`

D. `netsh ipsec dynamic show filteraction`

24. Dans le mode transport d'IPsec, quelle partie du paquet reste en clair (non chiffrée) ?

A. L'en-tête IP d'origine

B. Le corps du paquet

C. L'en-tête TCP

D. Les données de la couche application

25. Quel est l'inconvénient principal de l'authentification basée sur une clé pré-partagée dans IPsec ?

A. Moins sécurisé que RSA

B. Complexe à configurer manuellement

C. Nécessite une infrastructure PKI complète

D. Ne fonctionne qu'en mode tunnel

26. Quelle méthode d'authentification n'est pas supportée par IPsec ?

A. Certificats numériques

B. Mot de passe utilisateur

C. Clés pré-partagées

D. Clés publiques RSA

27. Quel algorithme est couramment utilisé dans IPSec pour vérifier l’intégrité des paquets lors d'une action de filtre d’authentification uniquement ?

A. MD5

B. AES

C. RSA

D. SHA1

28. Quel algorithme est couramment utilisé avec ESP dans IPSec pour le chiffrement des paquets ?

A. AES-128

B. 3DES

C. SHA256

D. MD5

29. Quel protocole IPsec fournit l'intégrité des données et l'authentification mais ne chiffre pas les paquets ?

A. ESP

B. AH

C. IKEv2

D. L2TP

30. Quel est l’avantage principal de l’utilisation de l’AES dans IPsec ?

A. Facilité d’implémentation

B. Amélioration des performances et de la sécurité

C. Compatibilité avec les systèmes anciens

D. Aucun