1. 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

2. 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"

3. 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

4. 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)

5. 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

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

A. OpenVPN

B. IKEv2/IPsec

C. PPTP

D. WireGuard

7. 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

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. 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

17. 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

18. 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`

19. 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

20. 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

21. 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

22. 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

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

A. AES-128

B. 3DES

C. SHA256

D. MD5

24. 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

25. 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

26. Quel est l’impact principal de l’augmentation de la taille d’une clé RSA à 4096 bits ?

A. Meilleure compatibilité

B. Amélioration significative de la performance

C. Sécurité accrue mais performance réduite

D. Aucune différence notable

27. Quel algorithme offre une sécurité similaire à RSA avec des clés beaucoup plus courtes ?

A. DES

B. ECDSA

C. Blowfish

D. AES

28. Quelle est la taille de clé RSA considérée comme le minimum acceptable pour garantir la sécurité des communications modernes ?

A. 512 bits

B. 1024 bits

C. 2048 bits

D. 8192 bits

29. Quel est l'avantage principal de l'utilisation d'ECDSA par rapport à RSA pour les communications sécurisées ?

A. Plus de compatibilité avec les anciens systèmes

B. Chiffrement plus rapide avec des clés plus courtes

C. Moins de sécurité que RSA

D. Meilleure intégration dans les protocoles SSL

30. Lors de la génération d’un certificat auto-signé, quelle taille de clé RSA est généralement recommandée pour un équilibre entre performance et sécurité ?

A. 512 bits

B. 1024 bits

C. 2048 bits

D. 8192 bits

31. Quel est l’impact principal de l’utilisation de clés RSA de 4096 bits par rapport à 2048 bits ?

A. Sécurité doublée avec les mêmes performances

B. Sécurité accrue mais performance dégradée

C. Aucune différence en termes de sécurité

D. Moins de compatibilité avec les navigateurs modernes

32. Quel algorithme est le plus souvent utilisé pour les certificats SSL/TLS dans les environnements nécessitant des performances optimales ?

A. RSA 4096 bits

B. ECDSA 256 bits

C. Blowfish

D. Triple DES

33. Si la taille d’une clé RSA est augmentée de 2048 bits à 4096 bits, quel aspect est principalement affecté ?

A. Le temps de chiffrement

B. La taille des certificats générés

C. La compatibilité avec les anciens navigateurs

D. La vitesse de négociation des connexions sécurisées