■ SDV Toolbox - Rapport de Sécurité

Outil:	Metasploit Framework
Date:	07/06/2025 à 16:43:10
Cible:	192.168.236.142:80
Opérateur:	SDV Security Team

■ Résultats de l'Exploitation Metasploit

■■ EXPLOITATION EXÉCUTÉE

Paramètre	Valeur
■ Module d'exploit	auxiliary/scanner/portscan/tcp
■ Cible (RHOST)	192.168.236.142
■ Port (RPORT)	80
■ Payload	Aucun
■ Date d'exploitation	07/06/2025 à 16:43:10
■■ Statut	Exploitation exécutée

■ Log détaillé de l'exploitation :

```
[*] Processing /tmp/tmptbtvzilz.rc for ERB directives.
resource (/tmp/tmptbtvzilz.rc)> use auxiliary/scanner/portscan/tcp
resource (/tmp/tmptbtvzilz.rc)> set RHOSTS 192.168.236.142
RHOSTS => 192.168.236.142
resource (/tmp/tmptbtvzilz.rc)> set RPORT 80
[!] Unknown datastore option: RPORT. Did you mean PORTS?
RPORT => 80
resource (/tmp/tmptbtvzilz.rc)> run
[+] 192.168.236.142:80 - 192.168.236.142:21 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:22 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:23 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:25 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:53 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:80 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:111 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:139 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:445 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:512 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:513 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:514 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:1099 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:1524 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:2049 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:2121 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:3306 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:3632 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:5432 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:5900 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:6000 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:6667 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:6697 - TCP OPEN
```

```
[+] 192.168.236.142:80 - 192.168.236.142:8009 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:8180 - TCP OPEN
[+] 192.168.236.142:80 - 192.168.236.142:8787 - TCP OPEN
[*] 192.168.236.142:80 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
resource (/tmp/tmptbtvzilz.rc)> exit
```

■■ Recommandations de sécurité :

• Aucune exploitation réussie détectée

• Continuez à surveiller la sécurité du système

• Maintenez tous les systèmes à jour avec les derniers correctifs

• Implémentez une stratégie de défense en profondeur

• Surveillez les connexions réseau anormales

• Effectuez des tests de pénétration réguliers

• Formez les équipes aux bonnes pratiques de sécurité

• Configurez des systèmes de détection d'intrusion (IDS/IPS)