

TP 10 Guillaume Sanchez

Exploitation de SMBv1 (EternalBlue)

Pour réaliser ce TP, j'ai choisi la vulnérabilité EternalBlue, Exploitation de SMBv1 que j'ai référencé dans le TP 8.

Il s'agit d'une faille critique exploitée par le Malware WannaCry. Elle exploite une faille de SMB1 et utilise le port TCP 445 et ce répond à travers le réseau local.

Schéma réseau

Voici comment sera positionné la sonde Snort :

Internet --- Routeur --- **Sonde Snort** --- Switch --- Machines internes

La sonde sera placée entre le routeur et le switch interne. Cela permettra d'analyser tout le trafic entrant et sortant vers les machines internes, donc de détecter les tentatives d'exploitation en provenance d'attaquant externes et les comportements de propagation sur le LAN.

Règle Snort pour EternalBlue (SMBv1 - CVE-2017-0144)

Voici la règle snort qui permettra de détecter une tentative d'exploitation SMBv1 selon la CVE-2017-0144 : <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144>

```
alert tcp any any -> any 445 (msg:"Tentative d'exploitation EternalBlue (SMBv1)";  
flow:to_server,established; content:"|00 00|"; offset:4; depth:2;  
reference:cve,2017-0144; classtype:attempted-admin; sid:1000001; rev:1;)
```

Explication de la règle :

- **alert tcp any any -> any 445** : surveille tout le trafic TCP entrant vers le port 445.
- **msg**: message d'alerte.
- **flow:to_server,established** : cible les connexions établies vers un serveur.
- **content:"|00 00|"; offset:4; depth:2** : vérifie une signature binaire présente dans l'entête SMB.
- **reference** : référence la faille CVE.
- **classtype** : type de menace.
- **sid** : identifiant unique.
- **rev** : version de la règle.

Cette règle a été choisie car elle permet de surveiller un vecteur d'entrée utilisé par WannaCry pour pénétrer le réseau. SMBv1 est encore activé sur certaines vieilles machines, donc ça mise en place sur un réseau qui utilisent encore cette version de SMB est vivement conseillé. L'exploitation d'EternalBlue se produit sans interaction de l'utilisateur. Le trafic SMB peut facilement se propager en interne sans être vu.