INSA

Exercices d'examen

Décembre 2014

Détection d'intrusion

Exercice 1 *(2 points)*

Question 1 : Expliquez à quoi correspond un « faux négatif » dans le domaine de la détection d'intrusion.

Question 2 : Est-il plus important de s'y intéresser qu'à un faux positif ?

Exercice 2 *(4 points)*

Voici deux signatures de détection d'intrusion réseau utilisables par le logiciel Snort pour détecter des flux réseaux présentant des caractéristiques spécifiques :

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Pirate propaganda";
content:"Host : "; content:"eveoganda.blogspot.fr|0d 0a|"; nocase; content:"GET";
http_method; classtype:gamification; sid:98765; rev:1;)

alert udp $HOME_NET any -> $HOME_NET 53 (msg:"Pirate propaganda dns request";
flow:to_server; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|09|eveoganda|08|blogspot|02|fr"; nocase; classtype:gamification;
sid:98766; rev:1;)
```

Question 1 *(1 point)* : Indiquez la caractéristique commune à ces 2 signatures et donc le type de flux que l'on souhaite identifier.

Question 2 *(2 points)* : Présentez à présent les 2 différents types de flux réseau que chaque signature permet de repérer dans la communication. Discutez les différences entre les types de détection permis par chacune de ces signatures.

Voici une autre signature de détection d'intrusion réseau extraite de la base des signatures Snort pour détecter un type de flux spécifique :

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone transfer UDP";
content:"|00 00 FC|"; offset:14; reference:arachnids,212; reference:cve,1999-0532;
reference:nessus,10595; classtype:attempted-recon; sid:1948; rev:7;)
```

Question 3 *(1 point)* : Expliquez quel type de communication on détecte via cette signature. Pourquoi lever une alerte immédiatement dès que le flux apparaît (sans même regarder le contenu du message) ?