Meno (čitateľne) a podpis : .......................................................

Dňa : .........................................................................................

# IPS specialist – poznatky

Proces:

1. Explain me (as a non-IT business manager) the role of IPS in the organization, its purpose and reasoning behind your work.

........................................................................................................................................  
  
........................................................................................................................................

1. Simply describe IPS deployment option:  
     
   ........................................................................................................................................  
     
   ........................................................................................................................................
2. What is IPS evasion, name/simply describe some techniques?   
     
   ........................................................................................................................................  
     
   ........................................................................................................................................

........................................................................................................................................

1. Describe IPS operations on specific ISO-OSI layers with examples   
     
   ........................................................................................................................................  
     
   ........................................................................................................................................

........................................................................................................................................

1. What are your preferred vendors for specific ISO-OSI layers?

.............................................................................................................................  
  
.............................................................................................................................

.............................................................................................................................  
  
.............................................................................................................................

1. What is false positive / negative?

.............................................................................................................................  
  
.............................................................................................................................

1. Describe rule-tuning options:

.............................................................................................................................  
  
.............................................................................................................................

1. Provide examples for inappropriate use of IPS:

.............................................................................................................................  
  
.............................................................................................................................

1. Provide description on integration with other infrastructure devices – examples, issues:

.............................................................................................................................  
  
.............................................................................................................................

**################################################**

**Write here results of tasks 1 – 6 (as many as you can). For each task describe:**

* **Identification of attacker / victim**
* **Activity type (portscan, server attack, client attack,...)**
* **What happened (i.e. including CVE missused, exploit used,...)**
* **Add snort signatures that you think may catch the malicious activity**
* **What would you do in case of spotting this activity in network?**

**PLEASE NOTE THAT FILES MAY CONTAIN MALICIOUS CONTENT AND HANDLE THEM WITH CARE.**

**Task 1:**

**Task 2:**

**Task 3:**

**Task 4:**

**Task 5:**

**Task 6:**