**Questionnaires 2019-2020 – Fabrice CRASNIER**

|  |  |
| --- | --- |
| Quel est l’impact d’un incident de sécurité informatique ? | |
|  | Une perte de disponibilité, |
|  | Une perte financière, |
|  | Un impact sur l’image, |
|  | Une perte d'un équipement informatique |

|  |  |
| --- | --- |
| Quelle est la signification du Spoofing en cybersécurité ? | |
|  | Une nouvelle forme de pêche à la truite |
|  | La recherche de renseignement dans le cyberespace |
|  | Une technique frauduleuse de récupération de données |
|  | Une usurpation d’identité |

|  |  |
| --- | --- |
| Le botnet « Mirai » déclenche des attaques de type ? | |
|  | Un rançongiciel (ransomware, cryptolocker) |
|  | Une attaque DDOS (Distributed Denial of Service attack) |
|  | Une attaque par dépassement de tampon (Buffer overflow) |
|  | Une attaque par vol de session (session hijacking) |

|  |  |
| --- | --- |
| Dans le Dark IOT,  l’Arduino Pro Mini est un microcontrôleur qui permet ? | |
|  | d’émuler un USB HID Keyboard, mouse, or joystick |
|  | d’activer une console pour injecter des commandes |
|  | Connaitre la température de l’environnement |
|  | Mettre en place une payload |

|  |  |
| --- | --- |
| Quelle est la signification de l’acronyme TOR ? | |
|  | Terms Of Reference |
|  | The Onion Router |
|  | Type of Relationship |
|  | Top of Riser |

|  |  |
| --- | --- |
| Pour mettre en place une politique de sécurité du système d’information ? | |
|  | Je fais appel à une société qualifiée PASSI |
|  | Je fais appel à une société qualifiée PRIS |
|  | Je fais appel à une société qualifiée PDIS |
|  | Je suis les prescriptions EBIOS et ISO 27000 et suivants |

|  |  |
| --- | --- |
| Dans les activités PSID et PRIS que représente un IOC ? | |
|  | Inversion de contrôle |
|  | Indicateur de compromission |
|  | Independent Operating Company |
|  | Indian Oil Corporation |

|  |  |
| --- | --- |
| Dans le cadre d’une activité forensic, l’expert peut : | |
|  | Apporter son concours à la justice |
|  | Traiter des litiges entre professionnels |
|  | Mettre des personnes en garde à vue |
|  | Recueillir des preuves numériques |

|  |  |
| --- | --- |
| Face à une cyberattaque, en tant qu’utilisateur chevronné : | |
|  | Je commence à faire des investigations sur la machine infectée |
|  | Je panique et je pars rapidement en laissant le problème derrière moi |
|  | Je suis les directives d’urgence mises en place par la D.S.I. |
|  | J’éteins mon poste de travail |

|  |
| --- |
| Quelles mesures conservatoires prendre au sein du SI ? |
|  |

**REPONSE Questionnaires 2019-2020 – Fabrice CRASNIER**

|  |  |
| --- | --- |
| Quel est l’impact d’un incident de sécurité informatique ? | |
| X | Une perte de disponibilité, |
| X | Une perte financière, |
| X | Un impact sur l’image, |
|  | Une perte d'un équipement informatique |

|  |  |
| --- | --- |
| Quelle est la signification du Spoofing en cybersécurité ? | |
|  | Une nouvelle forme de pêche à la truite |
|  | La recherche de renseignement dans le cyberespace |
| X | Une technique frauduleuse de récupération de données |
| X | Une usurpation d’identité |

|  |  |
| --- | --- |
| Le botnet « Mirai » déclenche des attaques de type ? | |
|  | Un rançongiciel (ransomware, cryptolocker) |
| X | Une attaque DDOS (Distributed Denial of Service attack) |
|  | Une attaque par dépassement de tampon (Buffer overflow) |
|  | Une attaque par vol de session (session hijacking) |

|  |  |
| --- | --- |
| Dans le Dark IOT,  l’Arduino Pro Mini est un microcontrôleur qui permet ? | |
| X | d’émuler un USB HID Keyboard, mouse, or joystick |
| X | d’activer une console pour injecter des commandes |
|  | Connaitre la température de l’environnement |
| X | Mettre en place une payload |

|  |  |
| --- | --- |
| Quelle est la signification de l’acronyme TOR ? | |
|  | Terms Of Reference |
| X | The Onion Router |
|  | Type of Relationship |
|  | Top of Riser |

|  |  |
| --- | --- |
| Pour mettre en place une politique de sécurité du système d’information ? | |
| X | Je fais appel à une société qualifiée PASSI |
|  | Je fais appel à une société qualifiée PRIS |
|  | Je fais appel à une société qualifiée PDIS |
| X | Je suis les prescriptions EBIOS et ISO 27000 et suivants |

|  |  |
| --- | --- |
| Dans les activités PSID et PRIS que représente un IOC ? | |
|  | Inversion de contrôle |
| X | Indicateur de compromission |
|  | Independent Operating Company |
|  | Indian Oil Corporation |

|  |  |
| --- | --- |
| Dans le cadre d’une activité forensic, l’expert peut : | |
| X | Apporter son concours à la justice |
| X | Traiter des litiges entre professionnels |
|  | Mettre des personnes en garde à vue |
| X | Recueillir des preuves numériques |

|  |  |
| --- | --- |
| Face à une cyberattaque, en tant qu’utilisateur chevronné : | |
|  | Je commence à faire des investigations sur la machine infectée |
|  | Je panique et je pars rapidement en laissant le problème derrière moi |
| X | Je suis les directives d’urgence mises en place par la D.S.I. |
|  | J’éteins mon poste de travail |

|  |
| --- |
| Quelles mesures conservatoires prendre au sein du SI ? |
| * **Confiner :** mettre en quarantaine les postes informatiques * **Isoler :** couper tous les accès réseaux pour stopper l’incident ; * **Sauvegarder :** les journaux d’activités * **Collecter les renseignements internes :** auprès des 1ères personnes * **Collecter les renseignements externes :** auprès des prestataires * **Communiquer** |