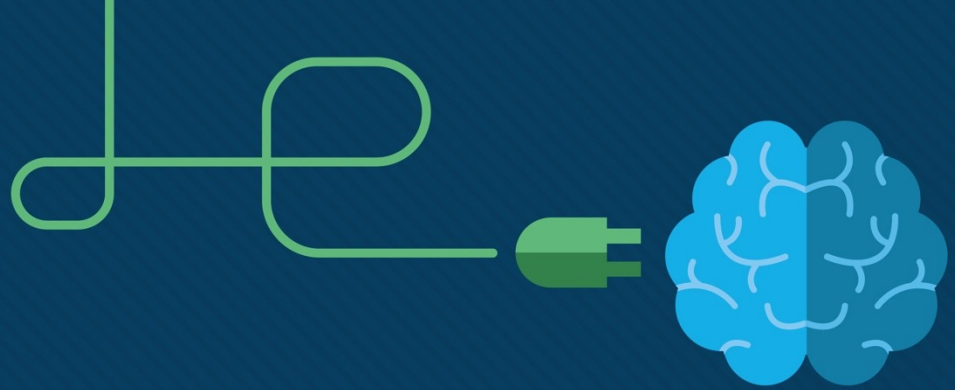


Module 1: Le danger

CyberOps Associate v1.0

Objectifs du module

Titre du module: Le danger

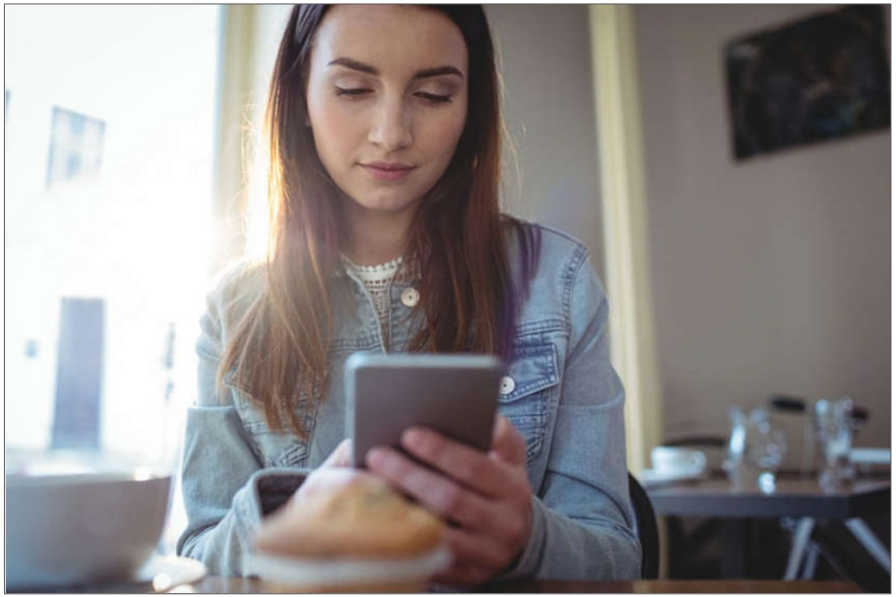
Objectif du Module: Expliquer pourquoi les réseaux et les données sont attaqués.

Titre du Rubrique	Objectif du Rubrique
Histoires de guerre	Expliquer pourquoi les réseaux et les données sont la cible d'attaques.
Hackers	Expliquer les raisons qui motivent les hackers à l'origine d'incidents de sécurité spécifiques.
Impact de la menace	Expliquer l'impact potentiel des attaques du réseau.

1.1 Histoires de guerre

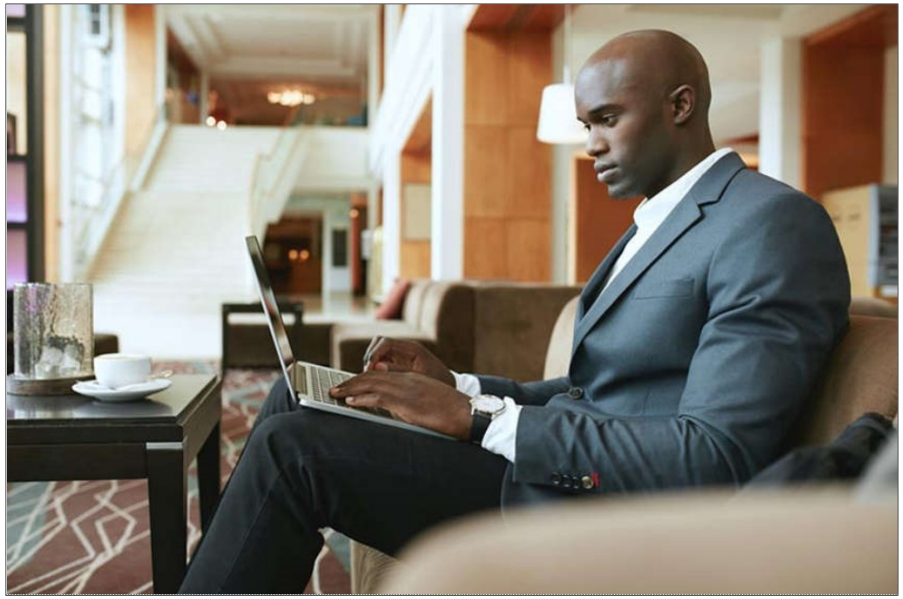
Détournement de personnes

- Un attaquant configure un point d'accès public ouvert sans fil non autorisé qui se fait passer pour un réseau sans fil légitime.
- Les points d'accès sans fil non fiables sont également connus sous le nom de points d'accès «evil twin».



Entreprises rançonnées

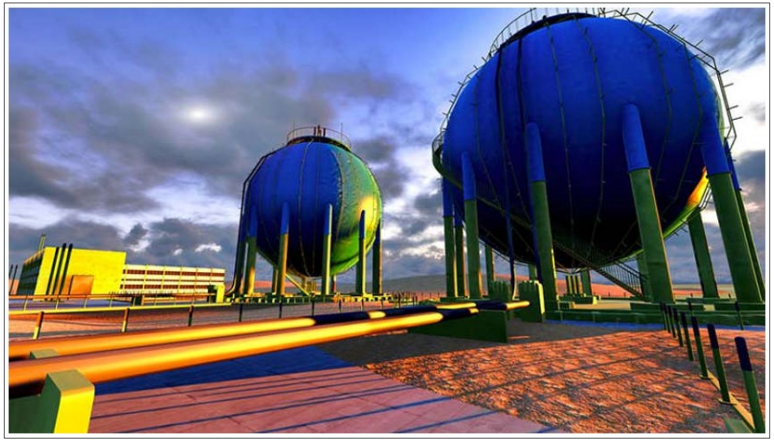
- Les employés d'une organisation sont souvent attirés par l'ouverture de pièces jointes qui installent de ransomware sur les ordinateurs des employés.
- Ce ransomware s'installe sur leur ordinateur et commence à collecter et à chiffrer les informations de l'entreprise.
- Les hackers sont clairement intéressés par les gains financiers, parce qu'ils conservent les données de l'entreprise jusqu'à ce qu'une rançon leur soit versée.



Pays ciblés

- Certains malwares actuels sont tellement sophistiqués

  et coûteux à créer que les experts en sécurité estiment que seul un pays ou un groupe de pays pourrait avoir l'influence et les fonds nécessaires pour le développer.
- Ces programmes malveillants peuvent viser les infrastructures vulnérables d'une nation, comme le système d'eau ou d'électricité.
- Un de ces logiciels malveillants était le ver Stuxnet qui infectait les lecteurs USB et infiltrait les systèmes d'exploitation Windows. Elle a ensuite ciblé le logiciel Step 7, développé par Siemens pour ses automates programmables (PLC).



Vidéo - Anatomie d'une attaque

Regardez cette vidéo pour voir les détails d'une attaque complexe.

Travaux pratiques - Installation d'une machine virtuelle

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Mettre en œuvre VirtualBox sur votre ordinateur personnel.
- téléchargerez et installerez ensuite le poste de travail CyberOps VM.

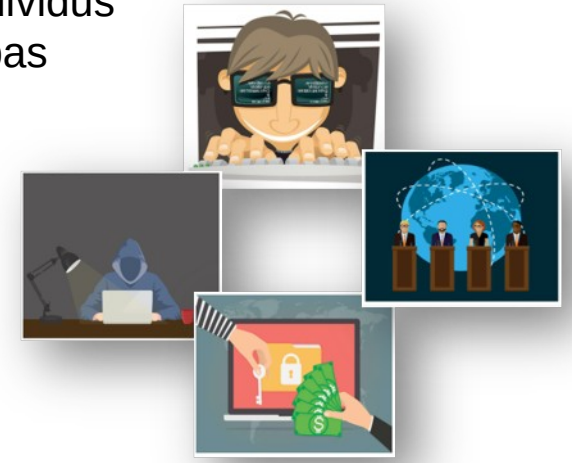
Travaux pratiques - Études de cas relatives à la cybersécurité

Lors de ces travaux pratiques, vous analyserez les cas mentionnés et vous répondrez à des questions.

1.2 Acteurs de menace

Acteurs de menace

- Les acteurs de menace sont des individus ou un groupe d'individus qui exécutent des cyber-attaques. Ils incluent, mais ne sont pas limités à :
  - Amateurs
  - Les hacktivistes
  - Groupe de crime organisé
  - Groupe de sponsorisé par l'État
  - Groupes terroristes
- Les cyber-attaques sont des actes intentionnels et malveillants destinés à nuire à une autre personne ou une entreprise.



Acteurs de menace (suite)

Amateurs

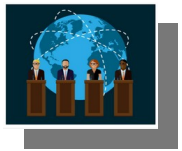
- Il sont également connus sous le nom de script kiddies, sont peu ou pas du tout expérimentés.
- Ils utilisent souvent des outils ou des instructions trouvées sur Internet pour lancer des attaques.
- Même s'ils utilisent des outils basiques, les résultats peuvent être dévastateurs.

Les hacktivistes

- Ils sont des hackers qui protestent contre diverses idées politiques et sociales.
- Ils publient des articles et des vidéos, en divulguant des informations sensibles et en perturbant des services web avec du trafic illégitime par l'intermédiaire d'attaques par déni de service distribué (DDoS).

Gains financiers

- La majorité des cybercriminels qui menacent constamment notre sécurité sont motivés par l'appât du gain.
- Les cybercriminels tentent d'accéder à nos comptes bancaires, à nos données personnelles et à toute autre information dont ils peuvent tirer parti pour gagner de l'argent.



Secrets commerciaux et politiques mondiales

- Parfois, les États-nations piratent d'autres pays ou interviennent dans leur politique interne.
- Les États utilisent le cyberespace à des fins d'espionnage industriel.
- Le vol de propriété intellectuelle peut offrir à un pays un avantage significatif sur le

L'internet des objets est-il protégé?

- L'IoT permet aux utilisateurs de connecter des objets pour améliorer leur qualité de vie.
- De nombreux appareils sur Internet ne contiennent pas
  le dernier micrologiciel. Certains appareils plus anciens ne sont même pas mis à jour pour intégrer des correctifs. Ces deux situations créent des opportunités pour les hackers et mettent en péril la sécurité des propriétaires de ces appareils.

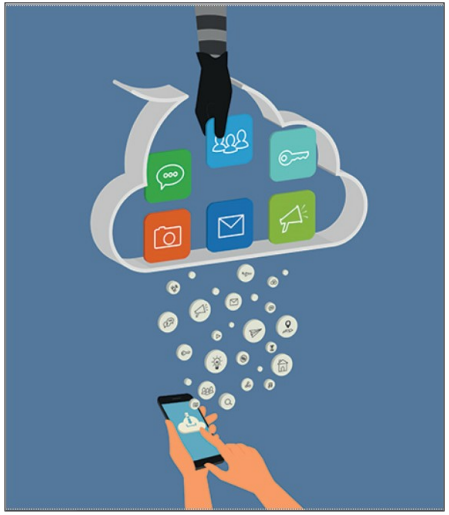
Travaux pratiques - Apprendre les détails des attaques

Dans cet atelier, vous rechercherez et analyserez les vulnérabilités des applications IoT.

1.3 Impact des menaces

PII, PHI, et PSI

- Les informations personnelles identifiables (PII) correspondent à l'ensemble des informations
  qui permettent d'identifier un individu, tels que le nom et le numéro de sécurité sociale.
- Les cybercriminels s'adonnent à une activité très lucrative: récupérer des listes d'informations PII qui peuvent ensuite être vendues sur le dark web. Ils peuvent utiliser les PII volées pour créer de faux comptes, tels que des cartes de crédit et des prêts à court terme.
- La communauté médicale crée et tient à jour
  des dossiers médicaux électroniques (EMRs) qui contiennent des informations
  PHI, un sous-ensemble de PII.
- PSI comprend les noms d'utilisateur, mots de passe et autres informations liées à la sécurité que les personnes utilisent pour accéder à des informations ou à des services sur le réseau.



Perte de l'avantage concurrentiel

- La perte de propriété intellectuelle pour les concurrents est une grave préoccupation.
- Elles redoutent également de perdre la confiance de leurs clients si elles étaient incapables de protéger leurs données personnelles.
- La perte de l'avantage concurrentiel est souvent plus liée à cette perte de confiance qu'au vol de secrets commerciaux par une autre entreprise ou un pays.

Politiques et sécurité nationale

- Les entreprises ne sont pas les seules à être piratées.
- Les hackers financés par un état peuvent perturber ou détruire des services et des ressources essentiels dans une nation ennemie.
- L'internet est devenu indispensable pour toute activité commerciale et financière. Perturber ces activités peut dévaster une économie nationale.

Travaux pratiques - Visualiser les chapeaux noirs

Dans cet atelier, vous rechercherez et analyserez les incidents de cybersécurité pour créer des scénarios dans lesquels les entreprises peuvent empêcher ou éradiquer une attaque.

1.4 Récapitulation : le danger

Qu'est ce que j'ai appris dans ce Module?

- Les acteurs de menace peuvent détourner des sessions bancaires et d'autres informations personnelles en utilisant des point d’accès public «Evil Twin».
- Parmi les hackers, on trouve notamment des amateurs, des hacktivistes, des groupes criminels organisés, des hackers financés par un état et des groupes terroristes.
- Au fur et à mesure que l'Internet des objets (IoT) se développe, les webcams, les routeurs et autres appareils dans nos foyers sont également attaqués.
- Les informations personnelles identifiables (PII) correspondent à l'ensemble des informations qui permettent d'identifier un individu.
- La communauté médicale crée et tient à jour des dossiers médicaux électroniques (EMRs) qui contiennent des informations PHI, un sous-ensemble de PII.
- PSI comprend les noms d'utilisateur, mots de passe et autres informations liées à la sécurité que les personnes utilisent pour accéder à des informations ou à des services sur le réseau.


CISCO