

Travail pratique #06



Objectifs

1. Inciter à se tenir au courant de l'actualité concernant la sécurité informatique
2. Comprendre et reproduire une faille logicielle
3. Comprendre le format utilisé par certaines sources d'information reliées aux failles informatiques
4. Acquérir des habitudes de veille en sécurité informatique
5. Explorer des concepts qui ne sont possiblement pas dans le contenu de cours tel que prévu initialement, mais tout de même pertinents

Instructions

Vous devez vous tenir informé des évènements qui se produisent en cours de session en rapport avec la sécurité informatique.

Vous devez documenter, reproduire et expliquer à vos collègues de classe une faille découverte (et annoncée publiquement) récemment (entre le début de la session et la date limite du travail). Vous devez m'informer de votre faille pour approbation, et aussi pour la réserver auprès de vos collègues de classe.

Lors de votre présentation en classe il sera important de :

1. Faire une présentation sommaire du logiciel affecté par la faille, surtout si ce logiciel est moins connu.
2. Expliquer la fiche descriptive (CVE, KB, email, forum, annonce officielle, etc) annonçant la faille. Mentionnez la date de découverte, le ou les nom(s) de ceux qui ont trouvé la faille, l'état de la faille (si elle est réglée ou non, temps de réponse, etc) et tout autre détails permettant d'établir le contexte de la faille.
3. Si applicable, reproduire la faille *live* devant la classe
4. Expliquer la faille et son fonctionnement. Si du code est disponible, en expliquer la partie critique et pertinente.
5. Montrer un cas d'exploitation de la faille si un *exploit* est disponible, sinon expliquer en détail comme l'exploiter. Si du code est disponible, en expliquer la partie critique et pertinente.
6. Expliquez le correctif à appliquer, et en quoi il règle le problème
7. Expliquez les impacts que cette faille a eu ainsi que ceux qu'elle aurait pu causer (*leak* d'informations personnelles, pertes/corruption de données, perte monétaires, atteinte à la réputation, etc)
8. Vous serez évalués sur le réalisme, la véracité et la clarté lors de votre présentation

9. Pour supporter visuellement votre présentation, veuillez utiliser un logiciel de présentation (power point, ou équivalent/mieux)
10. Seule contrainte par rapport à votre document de présentation : la première *slide* doit contenir vos noms, ainsi que le sujet de votre présentation. La dernière doit contenir vos références.

Voici quelques exemples de sources d'informations :

1. Site web d'un fabricant logiciel (firefox, chromium, wordpress, drupal, etc)
2. Liste des commits de projets populaires sur github
3. DSA : Debian Security Announce (<https://www.debian.org/security/>)
4. Microsoft Security Bulletin (<https://technet.microsoft.com/en-us/security/bulletin>)
5. CVE : Common Vulnerabilities and Exposure (<https://nvd.nist.gov/download/nvd-rss.xml>)
6. Forums dédiés à la sécurité
7. Site de nouvelles informatique/technologiques.
8. ...

Règles importantes

1. **Vous ne devez enfreindre aucune loi et/ou règles en vigueur du cégep**
2. Il s'agit d'un TP débouchant sur une présentation en classe, laquelle pouvant être faite à n'importe quel cours de la session avant la date de remise. Voir fichier `calendrier.txt` pour le détails des dates disponibles.
3. Maximum de 2 présentations par cours
4. Veuillez m'aviser au moins 3 jours à l'avance du cours dans lequel vous désirez faire votre présentation pour que j'ai le temps d'ajuster la matière du cours
5. Vous devez me faire approuver votre sujet avant de commencer
6. Ce travail est à faire en équipe de 2 ou 3 étudiants, planifiez vos équipes à l'avance pour ne pas vous retrouver seul
7. Votre présentation doit durer minimum 20 minutes et maximum 30 minutes. Elle se fera en utilisant votre propre portable que vous brancherez sur le projecteur.
8. Premier arrivé, premier servi. Deux équipes ne peuvent parler du même sujet.
9. Une écoute active lors de la présentation de vos collègues est importante. Des questions d'examens pourraient être formulées à partir de ce qui est présenté.

Remise

À remettre sur vortex **avant** le début de votre présentation (par un seul des membres de l'équipe) :

1. Votre présentation (powerpoint ou mieux)
2. Tout document pertinent que vous allez utiliser en classe pour la démonstration, demandez-moi pour être certain