Université Grenoble Alpes

Chap 3 : Outils spécifiques de cyber-sécurité

3. Cyber-menaces, cyber-réponses 2

EN LIGNE

- 3.1 Systèmes de Détection d'Intrusion et Systèmes de prévention d'intrusion
- 3.2 Honeypots (pots de miel)

HORS LIGNE

- 3.3 Analyse de vulnérabilités
- 3.4 Test de pénétration

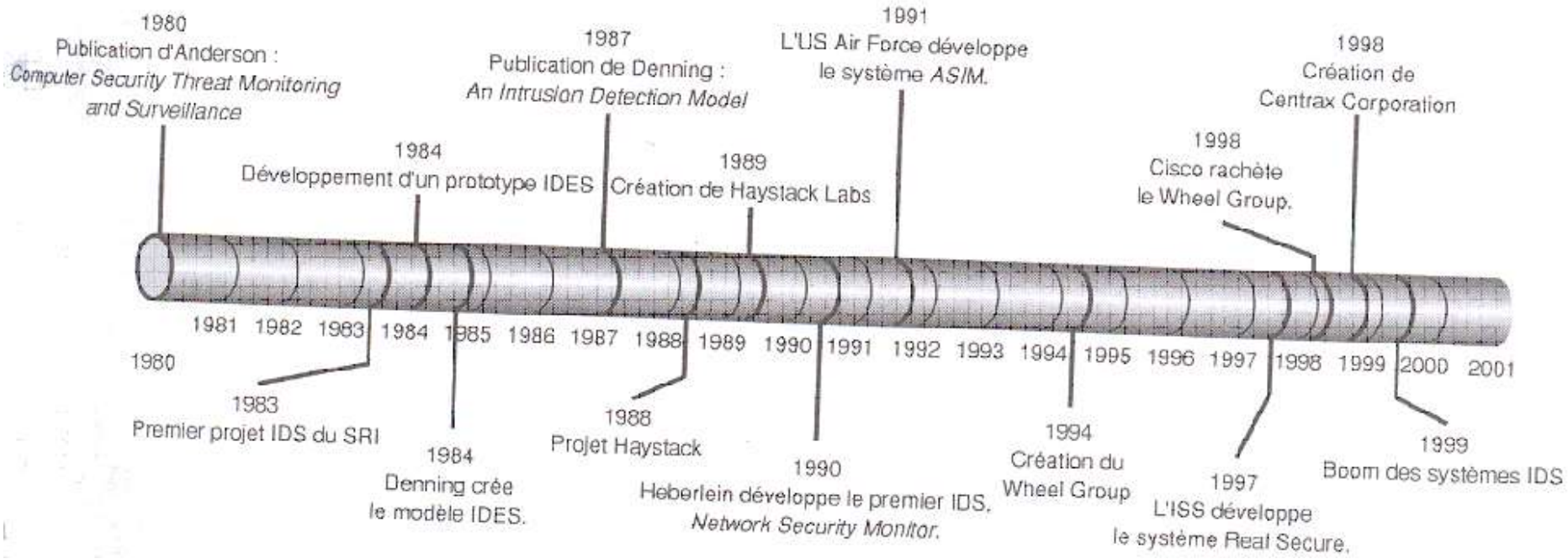
3.1 Détection d'intrusion et réponses

- Objectifs : détecter et répondre aux attaques réseaux et au code malveillant
- Code malveillant
  - Conçu pour nuire, perturber, ou empêcher l'ordinateur et le réseau de fonctionner (virus, chevaux de Troyes, vers…)
- Attaques de réseau
  - Attaques contre l'intégrité : changement non autorisé d'information
  - Attaque de reniement (répudiation) : démenti qu'un événement ou une transaction ait pu avoir lieu
  - Attaque de déni de service : actions ayant pour résultat l'indisponibilité des ressources et des services réseau
  - Attaques d'Accès : accès non autorisé aux ressources réseau

3.1 Mécanismes de détection d'intrusion

- Anti-virus
  - machines clientes
  - machines serveur (mail server…)
- Détection d'intrusion et réponses
  - Systèmes de surveillance pour la mise en évidence des intrusions ou de l'utilisation inapropriée et **répondre à** cette évidence
- Détection d'intrusion
  - Détection d'activité inapropriée, incorrecte ou anormale
- Réponse
  - Informer les parties concernées afin d'agir
    - Pour déterminer l'ampleur de la gravité d'un incident
    - Pour remédier aux effets de l'incident

3.1 Historique du développement des IDS



Aujourd'hui, les produits mettent en œuvre des concepts datant des années 1980

3.1 Types de systèmes de détections d'intrusions : NIDS (réseaux) (1/2)

- Network-based ID systems, Détection d'intrusion basée réseau (NIDS) : le NIDS réside sur un segment discret du réseau et surveille le trafic sur ce segment. Il consiste habituellement en un matériel réseau avec une carte réseau (NIC) qui *intercepte et analyse* les paquets réseau en temps réel. Les cartes d'interface réseau sont en général en mode promiscuité (*promiscuitous mode* => *écoute de tous les paquets*), elles sont alors en mode « furtif » afin qu'elles n'aient pas d'adresse IP.
  - Des paquets sont identifiés pour tester s'ils correspondent à une signature connue
    - **Signature de chaînes de texte (*string signature*)** : recherchez une chaîne de caractères qui indique une attaque possible
    - **signature de port** (***port signature***) : vérifier les tentatives de connexions vers les ports connus pour être la cible d'attaques fréquentes
    - **Signatures d'état d'en-tête** (***Header condition signature***) : recherche des combinaisons dangereuses ou illogiques dans les en-têtes de paquet

3.1 Types de systèmes de détections d'intrusions : NIDS (réseaux) (2/2)

- Généralement déployé devant et derrière les pare-feu et le VPN
- Caractéristiques
  - fournit une information fiable et en temps réel sans consommer de ressources réseau ou serveur
  - Passif quand il acquiert les données et analyse les paquets et les en-têtes
  - Peut détecter des attaques de dénis de service
  - Peut répondre à une attaque en cours pour réduire les dommages (grâce à la surveillance en temps réel)
  - Non capable de détecter des attaques contre un serveur fait par un intrus qui est loggé sur le terminal serveur

Comparison between firewall and IDS

Firewall

- Real-time
- Analysing each packet independently
- Action: If the packet does not fit with one of the ACL rules: the packet is dropped

IDS

- Real-time
- Analyse the packets AND make correlations between packets => detecting attack scenarios
- No action on the packets
- Action: for instance to close some « doors » on the system, to create a rules in the firewall ACLs

3.1 Types de systèmes de détections d'intrusions : HIDS (hôtes)

- Host-based ID systems (systèmes de détection d'intrusion basé sur l'hôte): utilise de petits programmes qui résident sur un hôte (serveur web, serveur messagerie…)
  - Supervise le système d'exploitation
  - Détecte les activités inapropriées
  - Écrit dans les fichiers de log (historiques)
  - Déclenche des alarmes
  - Caractéristiques
    - Supervise les accès et les modifications dans les fichiers système critiques et les modifications de privilèges des utilisateurs
    - Détecte les attaques de l'intérieur de manière plus efficace que les NIDS
    - Relativement efficace pour détecter les attaques extérieures
    - Peut être configuré pour analyser tous les paquets réseau, les tentatives de connexion, les tentatives de login sur la machine surpervisée

3.1 IDSs basés sur la signature

- *Signature-based IDSs*: signature ou stockage des attributs caractérisant une attaque
  - Avantages
    - Faible taux de fausses alarmes
    - Standardisé (généralement)
    - Compréhensible par le personnel de sécurité
  - Inconvénients
    - Peu efficace pour détecter les attaques lentes qui se déroulent sur une période longue
    - Seules les signatures stockées dans la base de données sont détectées
    - Les bases de connaissance ont besoin d'être maintenues et mises à jour régulièrement
    - Les attaques nouvelles ou uniques sont souvent non détectées
      - Et indétectables car dépendant du système d'exploitation, de la version, de la plate-forme, de l'application …

3.1 IDS basés sur anomalies ou le comportement

- *Statistical anomaly-based or behavior-based IDSs* : détecte dynamiquement les déviations par rapport aux motifs appris (comportement normal de l'utilisateur) et déclenche une alarme lorsqu'une tentative d'intrusion se déroule
- A besoin d'apprendre le profil d'utilisation normale (ce qui est difficile à déterminer)
  - Avantages
    - Peut s'adapter dynamiquement à une vulnérabilité nouvelle, unique ou originale
    - Moins dépendants du système d'exploitation que les IDS basés sur la connaissance
  - Inconvénients
    - Ne détecte pas une attaque qui ne modifie pas significativement les caractéristiques du système d'exploitation
    - Haut taux de fausses alarmes. Un haut niveau de faux positif est le défaut le plus commun des systèmes de détection d'intrusion basés sur le comportement
    - Le réseau peut être la victime d'une attaque durant la phase d'apprentissage des comportements « normaux »

3.1 Quelques considérations concernant les IDSs

- Plusieurs considérations doivent être prises en compte concernant l'efficacité des IDS :
  - Le besoin d'échanger et de corréler des données avec d'autres infrastructures de sécurité (diverses technologies et politiques)
  - L'augmentation constante du trafic réseau
  - Risques inhérents au fait de prendre des décisions inappropriées (réponse à une détection)
  - Attaques sur les IDS eux-mêmes
  - Manque d'évaluation objective des IDS, et de stratégie de tests

3.1 Performances d'un IDS

- TP (true positive, *vrai positif*) correspond aux attaques correctement identifiées
- FP (false positive, *faux positif*) correspond à du comportement authentique identifié comme malveillant
- TN (True Negative, *vrai négatif*) correspond au rejet correct du comportement authentique
- FN (False Negative) correspond aux attaques non détectées
- Deux métriques sont utilisées pour évaluer la performance des IDS
  - True Positive Rate/*Taux de Vrai Positif* TPR=TP/(TP+FN)
    => =1 si pas de Faux Négatif
  - False Positive Rate/*Taux de Faux Positif* FPR=FP/(FP+TN
    => =0 si pas de Faux Positif
- Une autre mesure importante est le nombre de violations signalées pour chaque attaque ou manipulation de l'opérateur

3.1 Fonctionnalités des IDS : Réponses aux intrusions détectées

- Réponses actives
  - Entreprendre une action agressive contre l'intrus
    - (! Attention à la légalité !)
  - Restructurer l'architecture du réseau
    - Isoler le système attaqué
    - Modifier les paramètres d'environnement qui ont permis à l'intrusion d'avoir lieu
  - Surveiller le système attaqué
    - Collecter des informations pour tenter de comprendre l'intrusion
    - Identifier l'auteur de l'intrusion et sa démarche
    - Identifier les failles de sécurité en place
- Réponses passives
  - Génération d'une alarme
  - Emission d'un message SMS à destination de l'administrateur

3.1 Systèmes de prévention d'intrusion (IPS: Intrusion Prevention System)

- Blocage des attaques le plus tôt possible
- Opèrent en conjonction avec les IDS
- IDS et IPS sont combinés dans un même équipement
- Trois techniques mises en œuvre pour neutraliser les attaques
  - *Sniping* : permet à l'IDS de mettre fin à une attaque supposée en utilisant un paquet TCP de réinitialisation (*reset*) ou un message ICMP d'inaccessibilité (*unreachable*)
  - *Shunning* : permet à l'IDS de configurer automatiquement le routeur préfiltrant ou le pare-feu pour que celui-ci rejette le trafic en fonction de ce que l'IDS a détecté, empêchant ainsi la connexion
  - *Blocking* : extension du "*shunning*" : ici l'IDS contacte le routeur ou le pare-feu et crée une liste de contrôle d'accès (ACL) pour bloquer l'adresse IP de l'attaquant

3.1 Produits IDS

- Peu de standard dans le domaine de l'IDS
- Snort, Suricata
- Bro (www.bro-ids.org)
- Cisco secure IDS
- Dragon sensor
- E-Trust IDS
- Billy Goat
- Enterasys

Université Grenoble Alpes

3.2 Honeypots (pots de miel)

3.2 But des honeypots (pots de miel)

- Supervise un mécanisme qui est utilisé pour :
  - Eloigner un hacker de ressources stratégiques
  - Fournir une indication précoce qu'une attaque se déroule
- Buts
  - Mode recherche
    - Collecte des informations sur les nouveaux types d'attaque
    - Tendances d'attaque
  - Mode production
    - Prévient les attaques
    - Détecte les attaques
    - Répond aux attaques

3.2 Honeypots (pots de miel)

- Prévenir les attaques
  - Ralentir ou empêcher les scans réalisés par des vers ou les attaques automatisées en surveillant les plages d'adresse inutilisées et en détectant les activités de scan
  - Détourner l'énergie d'un attaquant en l'attirant sur ce « pot de miel » pendant que l'attaque est détectée, analysée et traitée
- Détecter les attaques
  - Capacité de traiter des attaques nouvelles ou inconnues
  - Capacité de traiter du code polymorphique
  - Capacité de traiter des données cryptées
  - Permette de réduire la quantité de données à analyser par la capture uniquement des informations d'attaques
  - Capable de fonctionner avec IPV6
- Solutions courantes
  - Honeyd http://www.honeyd.org
  - Projet Honeynet http://www.honeypot.net

Université Grenoble Alpes

3.3 Outils d'analyse de vulnérabilités

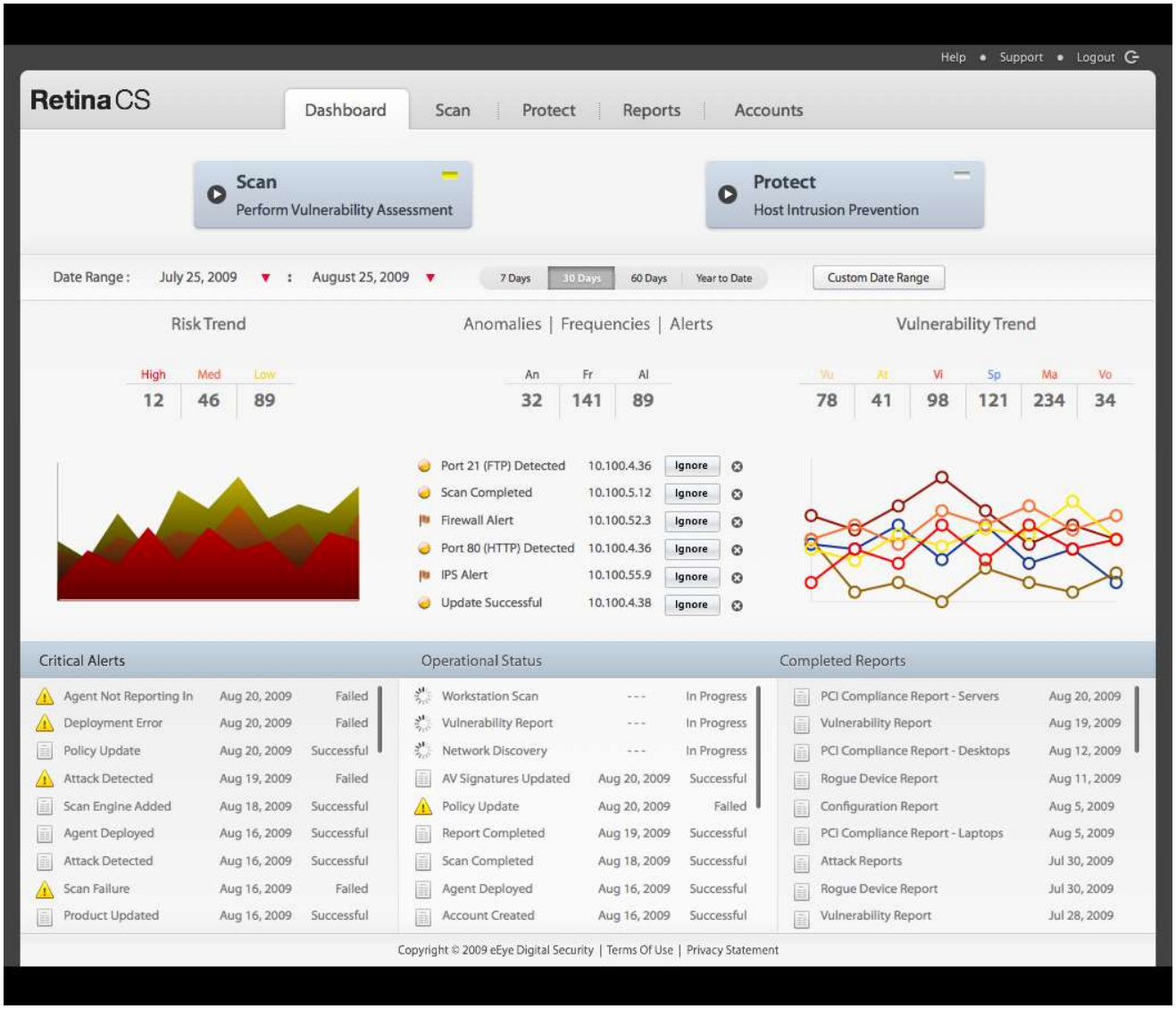
3.3 Outils d'analyse de vulnérabilités

- Scanner de sécurité distant
- Testent tous les services et tous les ports (sans faire de supposition sur les associations classiques services/ports)
- Précision des scans et détection
- Reporting
  - Nombreux liens avec une analyse complète des vulnérabilités
  - Niveau de risque que les vulnérabilités présentent pour le réseau
  - Graphiques
- Mise à jour des vulnérabilités
  - Mise à jour via des scripts qui peuvent être automatisés

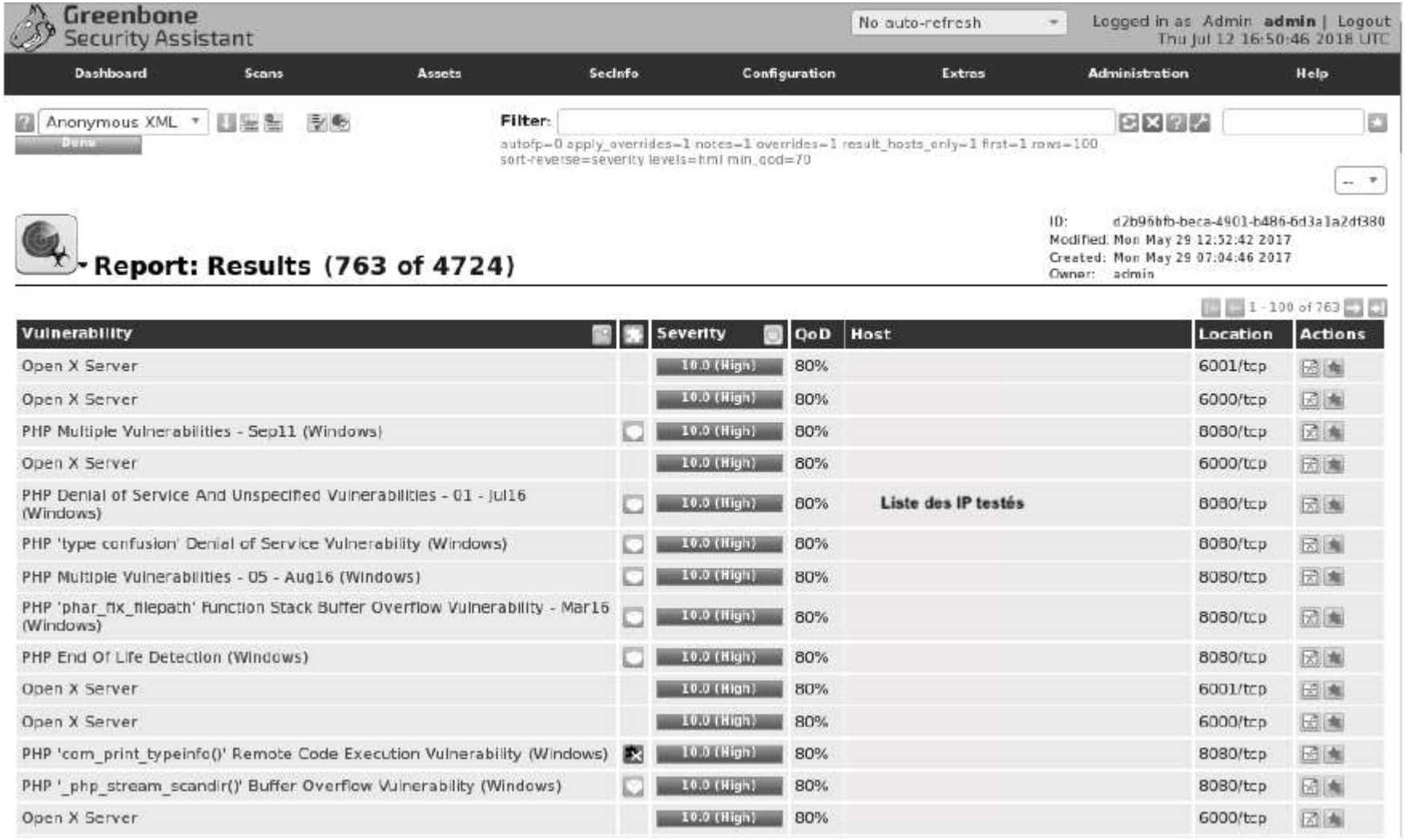
3.3 Outils d'analyse de vulnérabilités

- Exemple d'outils
  - Nessus: www.nessus.org, www.tenable.com
  - Retina : www.eeye.com
  - Open VAS : www.openvas.org
  - SAINT : http://saintcorporation.com
  - GFI Languard: www.gfi.com
  - Qualys FreeScan: www.qualys.com
  - Core Impact: www.coresecurity.com
  - MBSA: http://technet.microsoft.com
  - Wikto: www.sensepost.com
  - Nikto: http://cirt.net/niko2
  - WebInspect: http://download.spidynamics.com/webinspect/default.html
  - Acunetix: www.acunetix.com
  - SecurityMetrics (mobile) : www.securitymetrics.com
  - Retina for mobile: www.beyondtrust.com

3.3 Exemple de Retina



Exemple de vulnérabilités identifiées par OpenVas



3.3 Limites des scanners de vulnérabilité

- Donnent une assurance théorique de la sécurité
- Identifie les vulnérabilités, mais pas les conséquences du danger
- Produisent une longue liste de faiblesses (incluant des faux positifs)
- Ne permettent pas d'identifier les ressources susceptibles d'être compromises
- Ne peuvent simuler de véritables attaques
- N'explorent pas les relations de confiance entre les composants du réseau
- Ne démontrent pas les implications d'une attaque réussie

Université Grenoble Alpes

3.4 Outils de tests de pénétration

3.4 Outils de test de pénétration

- Interviennent là où les outils d'évaluation montrent leurs limites
- Ex : Core Impact
  - Core Security, www.coresecurity.com
  - Attaque les ressources informatiques et présente une analyse détaillées des risques encourus
  - Précision des scans et de la détection : permet d'explorer les ports et de détecter le système d'exploitation cible
  - Reporting :
    - Rapport de découverte : énumère tous les hôtes découverts et leurs vulnérabilités
    - Rapport d'historiques : énumère toutes les activités exécutées par l'utilisateur
- Mise à jour des vulnérabilités
  - Mise à jour des modules d'attaque
  - La société fait évoluer son produit

3.4 D’autres outils de pénétration

- Metasploit
- ExploitTree
- CANVAS

3. Conclusions

- On-line
  - NIDS, HIDS, si besoin et si possible
  - Honeypots
- Off-line
  - Analyse de vulnérabilités
  - Tests de pénétration
- Outils d'accompagnement pour les audits

3. Références bibliographiques

- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- MySQL, WebTraining, Jay Greenspan, OEM, 2002
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013
- E. Cole, R. Krutz, JW Conley - *Network security bible* – Wiley, 2005.
- Transparents C. Noblanc, 2009
- Thèse Oualid Koucham, Détection d'intrusions pour les systèmes de contrôle industriels, 2018, Univ. Grenoble Alpes
- Thèse Didier Pierrot, Détection dynamique des intrusions dans les systèmes informatiques, 2018, Univ. Lyon 2
- CEH, Certified Ethical Hacker, Matt Walker, MacGrawHill Eds, 2017.

- L’utilisation des méthodes et outils décrits dans ce cours engage la responsabilité des utilisateurs !