http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/lpro/cnms_en.html

M33-4. Cyber-threat, cyber-responses 2 : IDS

4. Cyber-threat, cyber-responses 2

ON-LINE SOFTWARE

- 4.1 Intrusion Detection Systems and Intrusion Prevention Systems
- 4.2 Honeypots

OFF-LINE SOFTWARE

- 4.3 Analysis of vulnerabilities
- 4.4 Test of penetration

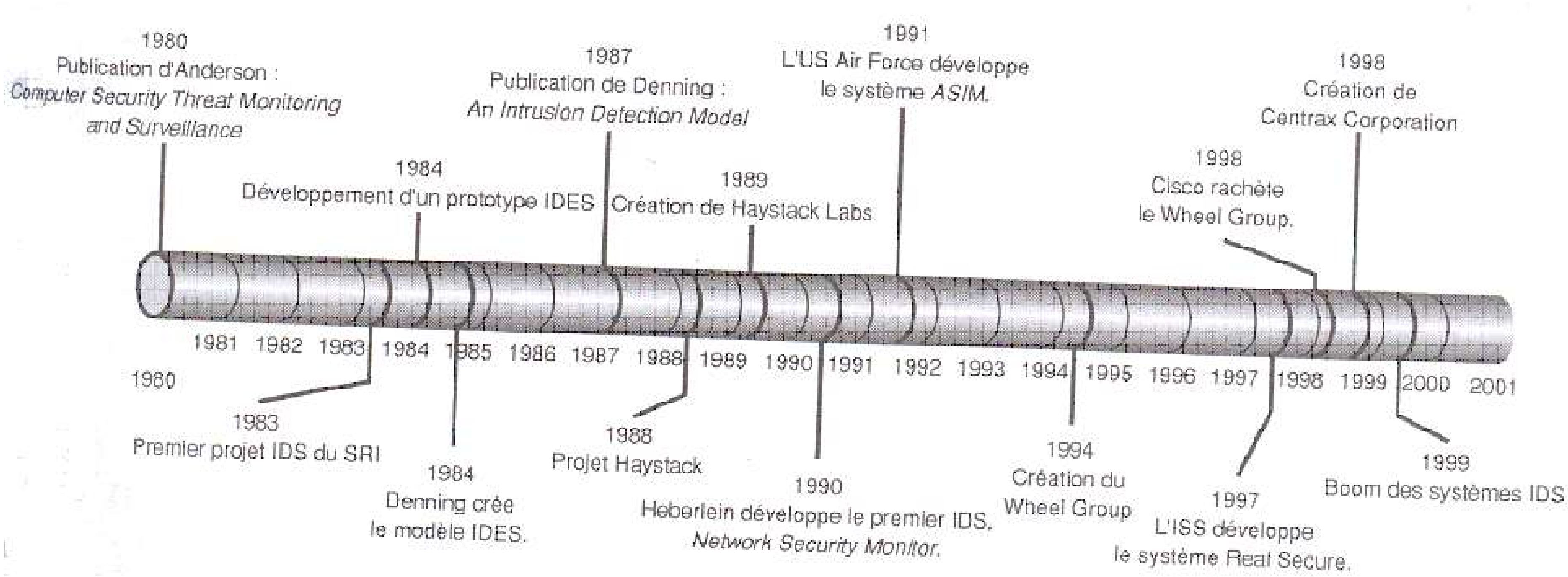
4.1 Intrusion detection and response

- Purpose: to detect and respond to network attacks and malicious code
- Malicious code
  - Intended to harm, disrupt, or circumvent computer and network functions (viruses, trojan horses, worms…)
- Network attacks
  - Modification attacks: unauthorized alteration of information
  - Repudiation attack: denial that an event or transaction ever occurred
  - Denial-of-service attack: actions resulting in the unavailability of network resources and services, when required
  - Access attacks: unauthorized access to network resources and information

4.1 Intrusion Detection Mechanisms

- Anti-virus
  - client machines
  - server machines (mail server…)
- Intrusion detection and response
  - Monitoring systems for evidence of intrusions or inappropriate usage and **responding** to this evidence
- ID
  - Detection of inappropriate, incorrect or anomalous activity
- Response
  - Notifying the appropriate parties to take action
    - To determine the extent of the severity of an incident
    - To remediate the incident’s effects

4.1 History of the development of IDS



1980
Publication d'Anderson :
Computer Security Threat Monitoring and Surveillance
1987
Publication de Denning :
An Intrusion Detection Model
1991
L'US Air Force développe le système *ASIM*.
1998
Création de Centrax Corporation
1984
Développement d'un prototype IDES
1989
Création de Haystack Labs
1998
Cisco rachète le Wheel Group.
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
1983
Premier projet IDS du SRI
1984
Denning crée le modèle IDES.
1988
Projet Haystack
1990
Heberlein développe le premier IDS, *Network Security Monitor*.
1994
Création du Wheel Group
1997
L'ISS développe le système Real Secure.
1999
Boom des systèmes IDS

Today, the products implement concepts dating from the years 1980

4.1 Types of ID systems: NIDS (1/2)

- Network-based ID systems (NIDSs, network IDSs): NIDS reside on a discrete network segment and monitor the traffic on that segment. They usually consist in a network appliance with a network interface card (NIC) that is *intercepting and analyzing* the network packets in *real time*. NIC are generally in promiscuous mode, this is a « furtive » mode in order not to use any IP address.
  - Packets are identified to be of interest if they match a signature
    - **String signature**: look for a text string that indicates a possible attack
    - **Port signature**: watch for connection attempts to well-known, frequently attacked ports
    - **Header condition signatures**: watch for dangerous or illogical combinations in packet headers

4.1 Types of ID systems: NIDS (2/2)

- Generally deployed in front or/and behind the firewalls and VPN
- Characteristics
  - provides reliable, real-time information without consuming network or host resources
  - Passive when acquiring data and review packets and headers
  - Can detect DoS attacks
  - Can respond to an attack in progress to limit damage (thanks to real-time monitoring)
  - Not able to detect attacks against a host made by an intruder who is logged in at the host's terminal

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 rule in the firewall ACLs

4.1 Types of ID systems: HIDS

- Host-based ID systems (host-based IDSs): use small programs that reside on a host computer (web server, mail server…)
  - Monitor the operating system
  - Detect inappropriate activity
  - Write to log files
  - Trigger alarms
  - Characteristics
    - Monitor accesses and changes to critical system files and changes in user privileges
    - Detect trusted insider attacks better than a network-based IDS
    - Relatively effective for detecting attacks from the outside
    - Can be configured to look at all the network packets, connection attempts, login attempts to the monitored machine, including dial-in attempts or other non-network-related communication ports

4.1 Signature-based or statistical anomaly-based IDSs

- Signature-based IDSs: signature or attributes that characterizes an attack are stored for reference (if there is a match, a response is initiated)
  - Advantages
    - Low false alarm rates
    - Standardized (generally)
    - Understandable by security personnel
  - Disadvantages
    - Failure to characterize slow attacks that extend over a long period of time
    - Only attack signatures that are stored in the database are detected
    - Knowledge database needs to be maintained and updated regularly
    - Because knowledge about attacks is very focused (dependent on the operating system, version, platform, and application), new, unique, or original attacks often go unnoticed

4.1 Signature-based or statistical anomaly-based IDSs

- Statistical anomaly-based or behavior-based IDSs: dynamically detects deviations from the learned patterns of « normal » user behaviour and trigger an alarm when an intrusive activity occurs
- Needs to learn the « normal » usage profile (which is difficult to determine)
  - Advantages
    - Can dynamically adapt to new, unique, or original vulnerabilities
    - Not as dependent upon specific operating systems as a knowledge-based IDS
  - Disadvantages
    - Does not detect an attack that does not significantly change the system-operating characteristics
    - High false alarm rates. High positive are the most common failure of behavior-based ID systems
    - The network may experienced an attack at the same time the intrusion detection system is learning the behaviour

4.1 Some IDSs issues

- Many issues confront the effective use of an IDS. These include the following:
  - The need to interoperate and correlate data accross infrastructure environments with diverse technologies and policies
  - Ever-increasing network traffic
  - Risks inherent in taking inappropriate automated response actions
  - Attacks on the IDSs themselves
  - The lack of objective IDS evaluation and test information

4.1 Performances of an IDS

- TP (True Positive) correspond to correctly identified attacks
- FP (False Positive) correspond to genuine behavior identified as malicious
- TN (True Negative) corresponds to the correct rejection of genuine behavior
- FN (False Negative) corresponds to missed attacks
- Two metrics to evaluate an IDS performance
  - True Positive Rate TPR=TP/(TP+FN) => =1 if no False Negative
  - False Positive Rate FPR=FP/(FP+TN=> =0 if no False Positive
- Another important metric is the number of violations reported for every attack or operator manipulation

4.1 Functionalities of IDS: Responses to the detected intrusions

- Active answers
  - To undertake an aggressive action against the intruder
    - (! Attention with legality!)
  - To restructure the network architecture
    - To isolate the attacked system
    - To modify the environment parameters which made the intrusion possible
  - To supervise the attacked system
    - To collect information in order to understand the intrusion
    - To identify the author of the intrusion and his approach
    - To identify security failures
- Passive answers
  - Generation of an alarm
  - Emission of a SMS message towards the administrator

4.1 IPS: Intrusion Prevention Systems

- Blocking of the attacks as soon as possible
- Operate in conjunction with IDS
- IDS and IPS are combined in the same equipment
- Three techniques implemented to neutralize the attacks
  - Sniping: allows IDS to put an end to a supposed attack by using a rebootstrapping (*reset*) TCP package or an inaccessibility (*unreachable*) ICMP message
  - Shunning: allows IDS to automatically configure the pre-filtering router or the firewall so that this one rejects the traffic according to what the IDS detected, thus preventing connection
  - Blocking: extension of “shunning”: here IDS contacts the router or the firewall and creates an access control list (ACL) to block the IP address of the attacker

4.1 IDS products

- Few standard in the field of IDS
- Snort, Suricata
- Bro (www.bro-ids.org)
- Cisco secure IDS
- Dragon sensor
- E-Trust IDS
- Billy Goat
- Enterasys

4.2 Honeypots

4.2 Purpose of honeypots

- Monitoring mechanism that is used to:
  - Keep a hacker **away** of valuable resources
  - Provide an early indication of an attack
- Purposes
  - Research mode
    - Collects information on new and emerging threats
    - Attack trends
  - Production mode
    - Preventing attacks
    - Detecting attacks
    - Responding to attacks

4.2 Honeypots

- Preventing attacks
  - Slowing or impeding scans initiated by worms or automated attacks by monitoring unused IP space and detecting scanning activities
  - Consuming an attacker’s energy through interaction with a honeypot while the attack is detected, analyzed, and handled
- Detecting attacks
  - Ability to capture new and unknown attacks
  - Ability to capture polymorphic code
  - Ability to handle encrypted data
  - They are reducing the amount of data that has to be analysed by capturing only attack information
  - Capable of operating with IPV6
- Current solutions
  - Honeyd http://www.honeyd.org
  - Honeynet project http://www.honeypot.net

4.3 Tools for analysis of vulnerabilities

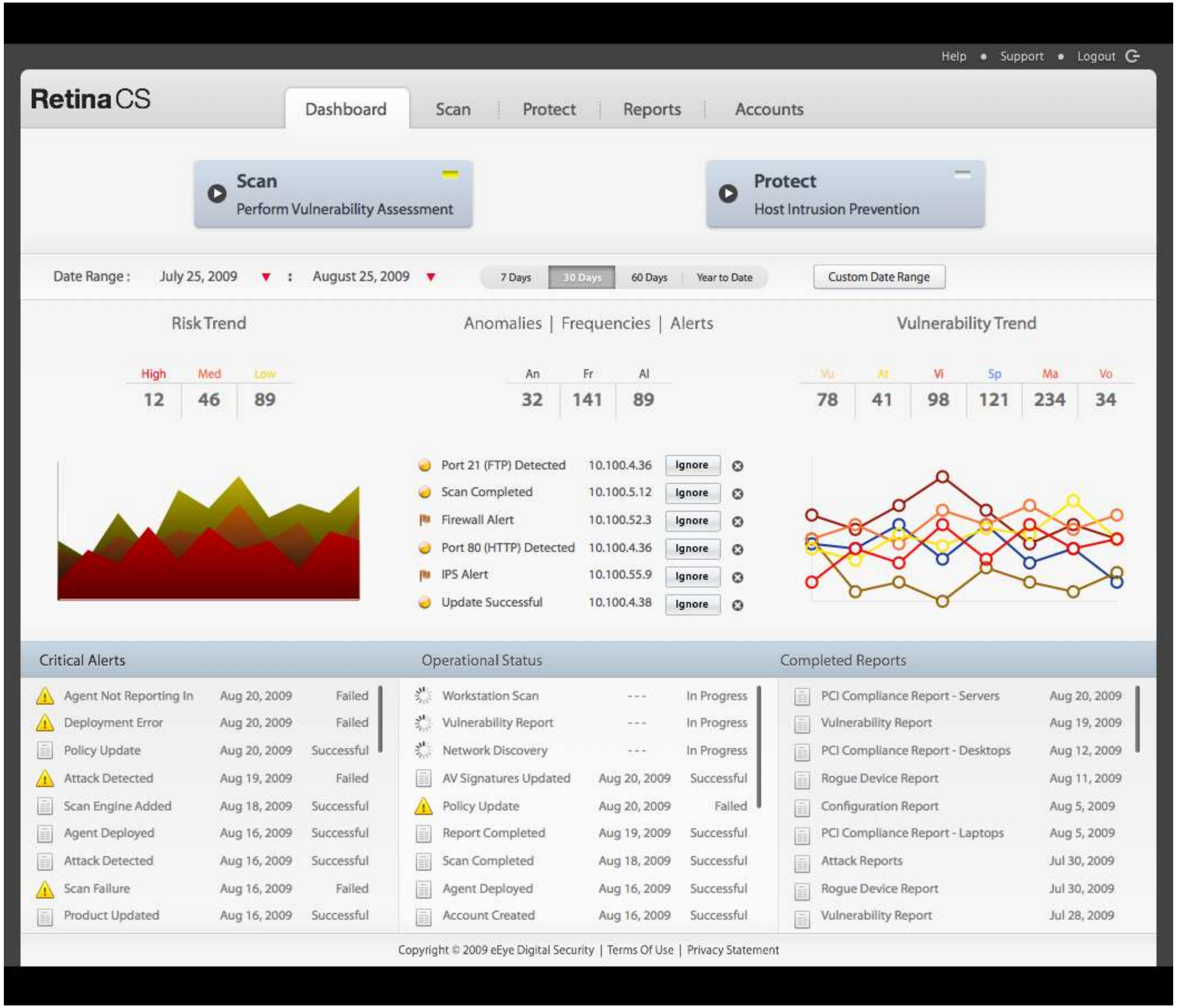
4.3 Tools for vulnerabilities analysis

- Distant security scanner
- test all the services and all the ports (without making assumption on traditional associations services/ports)
- Precision of the scans and detection
- Reporting
  - Many links with a complete analysis of vulnerabilities
  - risk Level which the vulnerabilities present for the network
  - Graphs
- Update of the vulnerabilities
  - Update via scripts which can be automated

4.3 Tools for vulnerabilities analysis

- Example of tools
  - 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

4.3 Example: Retina



Scan
Perform Vulnerability Assessment

Protect
Host Intrusion Prevention

Date Range : July 25, 2009 ▼ : August 25, 2009 ▼ | 7 Days | 30 Days | 60 Days | Year to Date | Custom Date Range

Risk Trend

High	Med	Low
12	46	89

Anomalies | Frequencies | Alerts

An	Fr	Al
32	141	89

Port 21 (FTP) Detected	10.100.4.36	Ignore
Scan Completed	10.100.5.12	Ignore
Firewall Alert	10.100.52.3	Ignore
Port 80 (HTTP) Detected	10.100.4.36	Ignore
IPS Alert	10.100.55.9	Ignore
Update Successful	10.100.4.38	Ignore

Vulnerability Trend

Vu	At	Vi	Sp	Ma	Vo
78	41	98	121	234	34

Critical Alerts

⚠ Agent Not Reporting In	Aug 20, 2009	Failed
⚠ Deployment Error	Aug 20, 2009	Failed
Policy Update	Aug 20, 2009	Successful
⚠ Attack Detected	Aug 19, 2009	Failed
Scan Engine Added	Aug 18, 2009	Successful
Agent Deployed	Aug 16, 2009	Successful
Attack Detected	Aug 16, 2009	Successful
⚠ Scan Failure	Aug 16, 2009	Failed
Product Updated	Aug 16, 2009	Successful

Operational Status

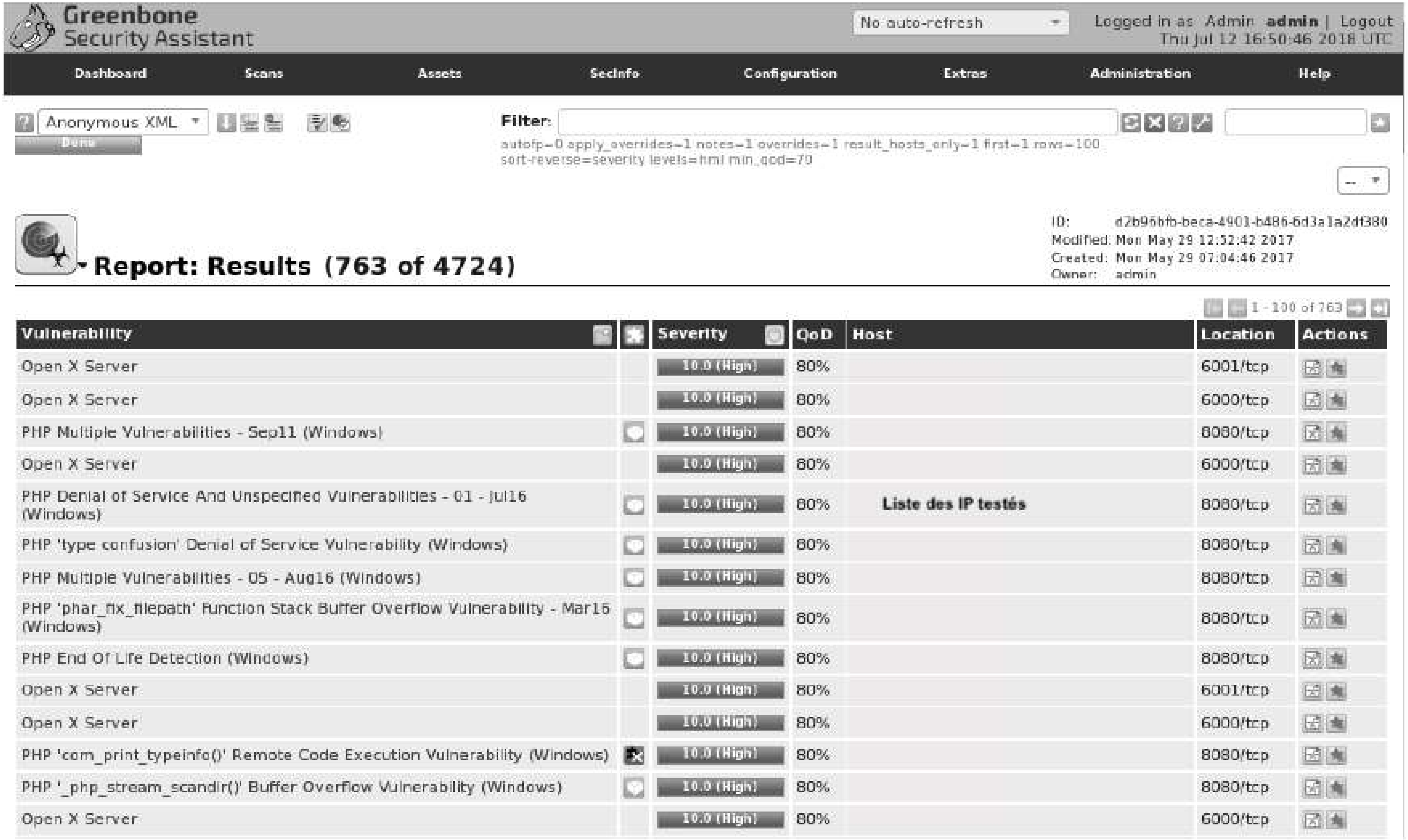
Workstation Scan	---	In Progress
Vulnerability Report	---	In Progress
Network Discovery	---	In Progress
AV Signatures Updated	Aug 20, 2009	Successful
⚠ Policy Update	Aug 20, 2009	Failed
Report Completed	Aug 19, 2009	Successful
Scan Completed	Aug 18, 2009	Successful
Agent Deployed	Aug 16, 2009	Successful
Account Created	Aug 16, 2009	Successful

Completed Reports

PCI Compliance Report - Servers	Aug 20, 2009
Vulnerability Report	Aug 19, 2009
PCI Compliance Report - Desktops	Aug 12, 2009
Rogue Device Report	Aug 11, 2009
Configuration Report	Aug 5, 2009
PCI Compliance Report - Laptops	Aug 5, 2009
Attack Reports	Jul 30, 2009
Rogue Device Report	Jul 30, 2009
Vulnerability Report	Jul 28, 2009

Copyright © 2009 eEye Digital Security | Terms Of Use | Privacy Statement

4.3 Example of vulnerabilities identified by OpenVas



autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (763 of 4724)

ID: d2b96bfb-beca-4901-b486-6d3a1a2df380
Modified: Mon May 29 12:52:42 2017
Created: Mon May 29 07:04:46 2017
Owner: admin

1 - 100 of 763

Vulnerability	Severity	QoD	Host	Location	Actions
Open X Server	10.0 (High)	80%		6001/tcp	
Open X Server	10.0 (High)	80%		6000/tcp	
PHP Multiple Vulnerabilities - Sep11 (Windows)	10.0 (High)	80%		8080/tcp	
Open X Server	10.0 (High)	80%		6000/tcp	
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)	10.0 (High)	80%	**Liste des IP testés**	8080/tcp	
PHP 'type confusion' Denial of Service Vulnerability (Windows)	10.0 (High)	80%		8080/tcp	
PHP Multiple Vulnerabilities - 05 - Aug16 (Windows)	10.0 (High)	80%		8080/tcp	
PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Windows)	10.0 (High)	80%		8080/tcp	
PHP End Of Life Detection (Windows)	10.0 (High)	80%		8080/tcp	
Open X Server	10.0 (High)	80%		6001/tcp	
Open X Server	10.0 (High)	80%		6000/tcp	
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability (Windows)	10.0 (High)	80%		8080/tcp	
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%		8080/tcp	
Open X Server	10.0 (High)	80%		6000/tcp	

4.3 Limits of the vulnerability scanners

- Give a theoretical insurance of security
- Identify the vulnerabilities, but not the consequences of the danger
- Produce a long list of weaknesses (including “false positive”)
- Do not allow to identify the resources likely to be compromised
- Cannot simulate true attacks

4.4 Tools for tests of penetration

4.4 Tools for test of penetration

- Intervene where the tools for evaluation show their limits
- Ex: Core Impact
  - Tackles the computer resources and presents a detailed analysis of the incurred risks
  - Precision of the scans and detection: allows to explore the ports and to detect the target operating system
  - Reporting:
    - Report of discovery: enumerate all the hosts discovered and their vulnerabilities
    - Report of histories: enumerate all the activities carried out by the user
- Update of the vulnerabilities
  - Update of the attack modules
  - The company makes evolve its product

4.4 Other penetration tools

- Metasploit
- ExploitTree
- CANVAS

4. Conclusions

- On-line
  - NIDS, HIDS, if needed and if possible
  - Honeypots
- Off-line
  - Vulnerability analysis
  - Penetration tests
- Tools usable for audits

4. Bibliographical references

- E. Cole, R. Krutz, JW Conley - *Network security bible* – Wiley, 2005.
- 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
- Slides C. Noblanc, 2009
- Thèse Oualid Koucham, ntrusion detection for industrial control systems, 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.

- The use of the methods and tools described in this course engages the responsibility for the users!