

3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo
CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
<http://rodolphe.ortalo.free.fr/ssi.html>

Plan (2/2)

- Protection utilisées dans la pratique
 - Protection réseau et *firewall*
 - Systèmes d'authentification
 - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
 - **Détection d'intrusion**
 - Audit, tests d'intrusion
 - Administration, exploitation et suivi de la sécurité
 - Observation et surveillance
- Protection des applications usuelles

Plan (détailé)

- **Détection d'intrusion**

- Terminologie
- Approches étudiées et tendances
- Mise en oeuvre
- Architecture
- Solutions (réseau)
 - Snort
 - Suricata
 - Bro-IDS, Prelude-IDS, Kismet, etc.
- Solution (hôte)
 - OSSEC HIDS
 - Samhain (Tripwire like)
- Traitement des alertes (problèmes, corrélation)
 - Prelude-IDS

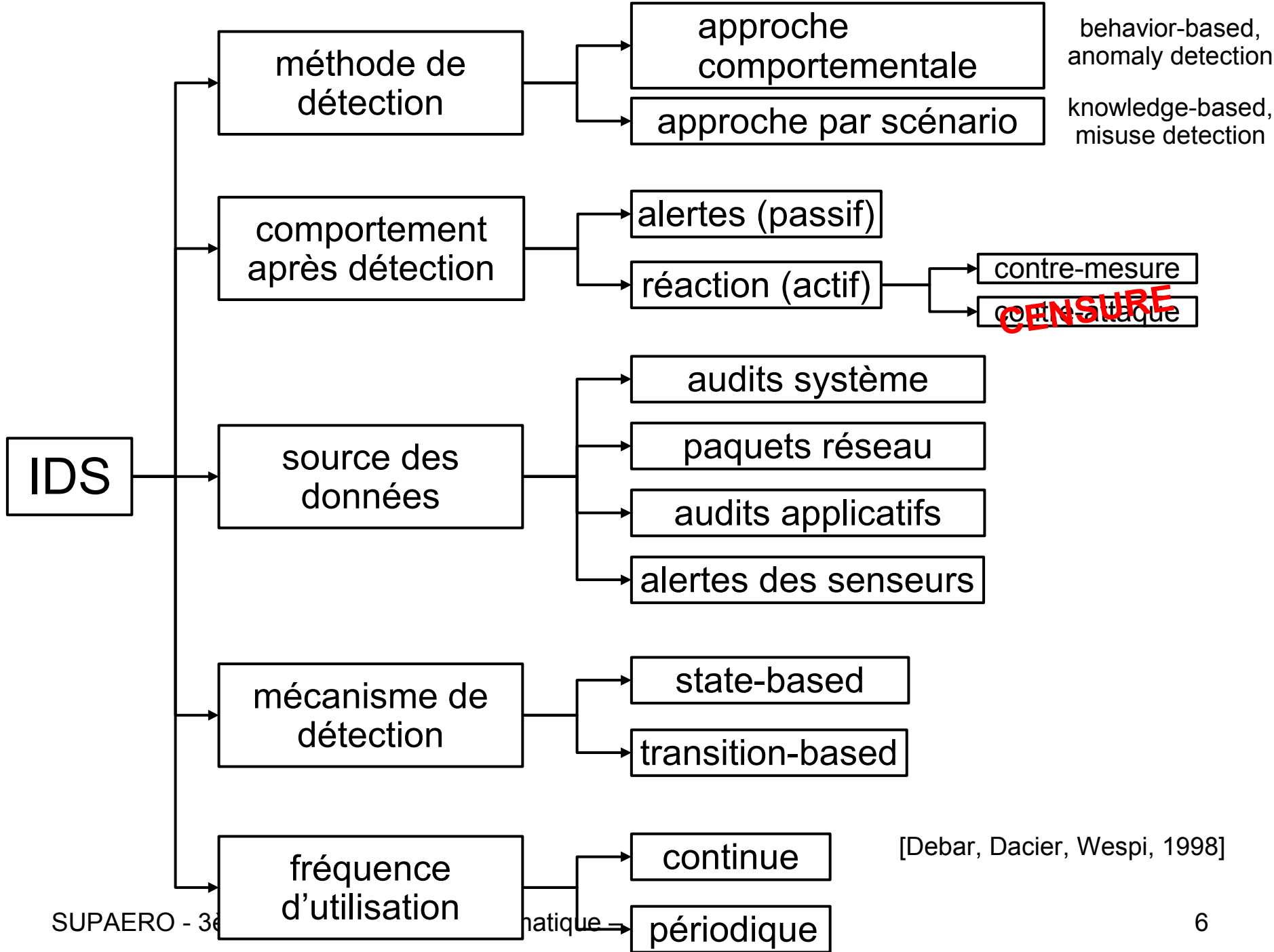


Vulnérabilités – Attaques – Alertes

- Vulnérabilités
 - Grande variété : *buffer overflow*, CGI, droits d'accès permissifs, interception de sessions réseaux, transferts de privilèges, *social engineering*, cryptanalyse, etc.
- « Attaque »
 - Exploitation d'une vulnérabilité
 - Attaque élémentaire ou scénario d'intrusion
 - Action malveillante ou suspecte
- Alertes
 - Message résultant de la détection d'une attaque
 - *IDMEF (XML): Intrusion Detection Message Exchange Format défini par l'IETF/IDWG*

Génération d'alertes (efficacité)

	Pas d'alerte	Alerte
Pas d'attaque	Vrai négatif 😊	Faux positif 😞
Attaque en cours	Faux négatif 😞	Vrai positif 😊



Techniques utilisables

- Approche par scénario
 - Systèmes experts (ES)
 - Analyse de signatures (SA)
 - Réseaux de Petri (PN)
- Approche comportementale
 - Statistiques (ST)
 - Systèmes experts (ES)
 - Réseaux neuronaux (NN)
 - Approche immunologique (UII)

Tendances actuelles

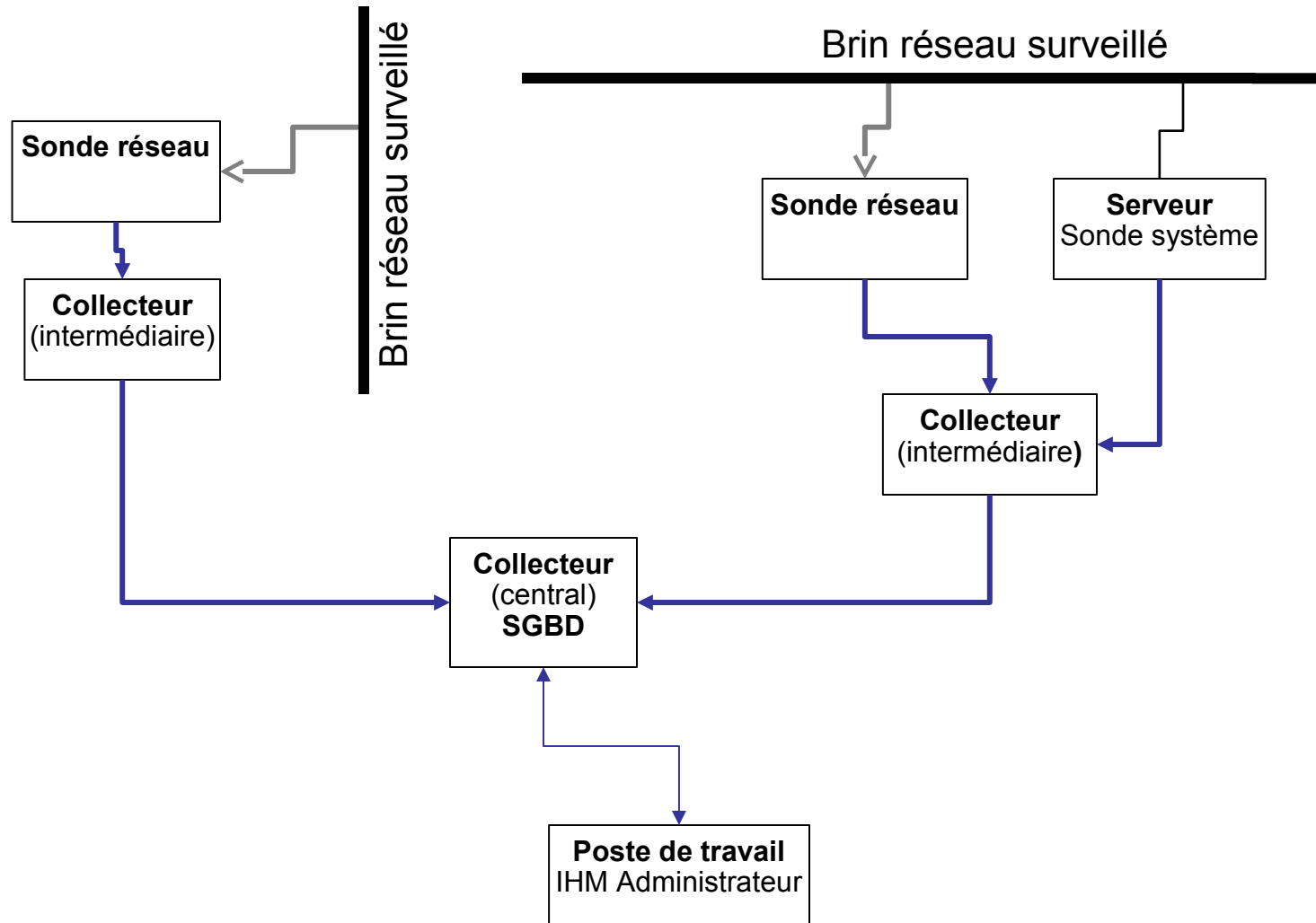
- Une seule technique par outil en général
- L'approche par signatures se généralise
 - Réalisation plus simple
 - Performances
- L'approche comportementale est peu utilisée par les outils commerciaux
- La réaction apparaît

- Un ou deux outils *open-source* par technique en général
- Des consoles plutôt commerciales voire infogérées

Mise en oeuvre

- Sondes
 - Observation du trafic
 - Positionnement
 - Problème des environnements commutés (*mirroring vs. taps*)
 - Sondes système
 - Nombre des signatures (et impact CPU)
 - Pertinence des signatures
- Consolidation des alertes
 - Collecteurs
 - Protocole d'échange sécurisé
 - Format d'échange IDMEF:
<http://www.ietf.org/html.charters/idwg-charter.html>

Architectures envisageables



Ex. : IHM ISS RealSecure

The screenshot displays the RealSecure Console interface. At the top, there is a menu bar (File, View, Window, Help) and a toolbar with various icons. Below the toolbar, the status bar shows 'Ready'. The main interface is divided into several panes:

- Activity Tree:** A tree view showing 'Active Events' with a list of event types, each with a status icon (minus, warning, or error):
 - HTTP_IIS3_Asp_Dot (minus)
 - FTP_Root (minus)
 - FTP_Pass (warning)
 - FTP_User (warning)
 - HTTP_Get (warning)
 - Windows_Null_Session (warning)
 - Netbios_Session_Granted (warning)
 - Netbios_Session_Request (warning)
 - POP_Password (warning)
 - POP_User (warning)
 - Rexec (warning)
- High Priority:** A table showing high-priority events.

Engine	Event	From	To	Info	Date
localhost	FTP_Root	208.21.2.92	208.21.2.38		Tue Ju
localhost	HTTP_IIS3_Asp_Dot	208.21.2.92	208.21.0.11	URL - /index..asp.	Tue Ju
- Medium Priority:** A table showing medium-priority events.

Engine	Event	From	To	Info	Date
localhost	FTP_User	208.21.2.92	208.21.2.38	USER - mark	
localhost	FTP_User	208.21.2.92	208.21.2.38	USER - root	
localhost	FTP_Pass	208.21.2.92	208.21.2.38	PASS - hello	
localhost	HTTP_Get	208.21.2.92	208.21.0.11	URL - /index%2e...	
- Low Priority:** A table showing low-priority events, currently empty.
- Engines:** A table showing the status of the security engines.

Engine	Location	Policy	Engine Status	Event Channel Status	Engine DB Progress
localhost	127.0.0.1	TestMax : MW000 - Fri Jun 19 08:27:21 1998	Active	Established. [ID=0xe7220028]	

Signatures – Snort (1)

SID	1800
Message	VIRUS Klez Incoming
Signature	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"VIRUS Klez Incoming"; flow:to_server,established; dsize:>120; content:"MIME"; content:"VGhpcyBwcm9"; classtype:misc-activity; sid:1800; rev:3;)
Summary	This event is generated when an incoming email containing the Klez worm is detected.
Impact	System compromise and further infection of target hosts.
Detailed Information	<p>W32/Klez.h@MM exploits the vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), enabling it to execute email attachments.</p> <p>Once executed, it can unload several processes including Anti-virus programs.</p> <p>The worm is able to propagate over the network by copying itself to network shares (assuming sufficient permissions exist). Target filenames are chosen randomly, and can have single or double file extensions.</p>
Affected Systems	Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2)
Attack Scenarios	This virus can be considered a blended threat. It mass-mails itself to email addresses found on the local system, then exploits a known vulnerability, spreads via network shares, infects executables on the local system.
Ease of Attack	Simple. This is worm activity.
False Positives	Certain binary file email attachments can trigger this alert.
False Negatives	None known.
Corrective Action	<p>Apply the appropriate vendor supplied patches.</p> <p>Block incoming attachments with .bat, .exe, .pif, and .scr extensions</p>
Contributors	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com>

Signatures – Snort (2)

SID	2251
Message	NETBIOS DCERPC Remote Activation bind attempt
Signature	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 135 (msg:"NETBIOS DCERPC Remote Activation bind attempt"; content:" 05 "; distance:0; within:1; content:" 0b "; distance:1; within:1; byte_test:1,&,1,0,relative; content:" B8 4A 9F 4D 1C 7D CF 11 86 1E 00 20 AF 6E 7C 57 "; distance:29; within:16; reference:cve,CAN-2003-0352; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/bulletin/MS03-026.asp; reference:cve,CAN-2003-0715; sid:2251; rev:1;)
Summary	This event is generated when an attempt is made to exploit a known vulnerability in Microsoft RPCSS service for RPC.
Impact	Denial of Service. Possible execution of arbitrary code leading to unauthorized remote administrative access.
Detailed Information	<p>A vulnerability exists in Microsoft RPCSS Service that handles RPC DCOM requests such that execution of arbitrary code or a Denial of Service condition can be issued against a host by sending malformed data via RPC.</p> <p>The Distributed Component Object Model (DCOM) handles DCOM requests sent by clients to a server using RPC. A malformed request to the host running the RPCSS service may result in a buffer overflow condition that will present the attacker with the opportunity to execute arbitrary code with the privileges of the local system account. Alternatively the attacker could also cause the RPC service to stop answering RPC requests and thus cause a Denial of Service condition to occur.</p>
Affected Systems	<p>Windows NT 4.0 Workstation and Server</p> <p>Windows NT 4.0 Terminal Server Edition</p> <p>Windows 2000</p> <p>Windows XP</p>

Prelude IDS Web Front-End - Filter builder [guest] - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ? Adresse http://tspsecur/piwi/Filters.pl?priv_name=&trigger=&pa

Alert List HeartBeat Top 20 Attackers Top 20 Attacks Statistics

Filter Factory Edit current filter None Load filter

Severity filter

- high
- medium
- low

Sort by

- timestamp
- group by key

Results per page

6

submit

Group by

- Classification
- Source address
- Target address
- Target port

Order

- Desc.
- Asc.






Since

1 month

<-- re-open sensor_tree

23 results for those filters. Page 4/4.

First Prev Last

P	Id	Classification	Impact	Completion	Source	Destination	Class	Timestamp
	1161	SIMPLE Windows Event ID [560]: security FAILURE	user	failed	unknown	50.128.146.178	Prelude LML/HIDS	2003-10-31 16:46:50
	1160	SIMPLE Windows Event ID [560]: security FAILURE	user	failed	unknown	50.128.146.178	Prelude LML/HIDS	2003-10-31 16:45:59
	1159	SSH Remote user logging	user	succeeded	50.128.146.178	127.0.0.1 22/tcp (ssh)	Prelude LML/HIDS	2003-10-31 16:48:33
	1158	SSH Remote user logging	user	succeeded	50.128.146.178	127.0.0.1 22/tcp (ssh)	Prelude LML/HIDS	2003-10-31 16:40:24
	1157	Root login	admin	succeeded	unknown	127.0.0.1	Prelude LML/HIDS	2003-10-31 16:35:27

Intranet local

Limites actuelles de la détection d'intrusion

- Faible taux de détection
 - Faux négatifs
- Trop d'alertes
 - Fausses alertes : Faux positifs
 - Plusieurs milliers d'alertes générées en une semaine
- Le niveau de granularité d'une alerte est trop faible
 - Pas de vision globale
 - Difficile de détecter une attaque distribuée
- Difficile de détecter les attaques nouvelles
 - C'est un avantage des approches comportementales

Signatures – Snort (1)

SID	1800
Message	VIRUS Klez Incoming
Signature	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"VIRUS Klez Incoming"; flow:to_server,established; dsize:>120; content:"MIME"; content:"VGhpcyBwcm9"; classtype:misc-activity; sid:1800; rev:3;)
Summary	This event is generated when an incoming email containing the Klez worm is detected.
Impact	System compromise and further infection of target hosts.
Detailed Information	<p>W32/Klez.h@MM exploits the vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), enabling it to execute email attachments.</p> <p>Once executed, it can unload several processes including Anti-virus programs.</p> <p>The worm is able to propagate over the network by copying itself to network shares (assuming sufficient permissions exist). Target filenames are chosen randomly, and can have single or double file extensions.</p>
Affected Systems	Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2)
Attack Scenarios	This virus can be considered a blended threat. It mass-mails itself to email addresses found on the local system, then exploits a known vulnerability, spreads via network shares, infects executables on the local system.
Ease of Attack	Simple. This is worm activity.
False Positives	Certain binary file email attachments can trigger this alert.
False Negatives	None known.
Corrective Action	<p>Apply the appropriate vendor supplied patches.</p> <p>Block incoming attachments with .bat, .exe, .pif, and .scr extensions</p>
Contributors	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com>

SID:1800

deleted.rules:

```
# alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25  
(msg:"DELETED VIRUS Klez Incoming";  
flow:to_server,established; dsize:>120;  
content:"MIME";  
content:"VGhpcyBwcm9";  
classtype:misc-activity;  
sid:1800; rev:6;)
```

Signature désormais désactivée

Signatures – Snort (2)

SID	2251
Message	NETBIOS DCERPC Remote Activation bind attempt
Signature	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 135 (msg:"NETBIOS DCERPC Remote Activation bind attempt"; content:" 05 "; distance:0; within:1; content:" 0b "; distance:1; within:1; byte_test:1,&,1,0,relative; content:" B8 4A 9F 4D 1C 7D CF 11 86 1E 00 20 AF 6E 7C 57 "; distance:29; within:16; reference:cve,CAN-2003-0352; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/bulletin/MS03-026.asp; reference:cve,CAN-2003-0715; sid:2251; rev:1;)
Summary	This event is generated when an attempt is made to exploit a known vulnerability in Microsoft RPCSS service for RPC.
Impact	Denial of Service. Possible execution of arbitrary code leading to unauthorized remote administrative access.
Detailed Information	<p>A vulnerability exists in Microsoft RPCSS Service that handles RPC DCOM requests such that execution of arbitrary code or a Denial of Service condition can be issued against a host by sending malformed data via RPC.</p> <p>The Distributed Component Object Model (DCOM) handles DCOM requests sent by clients to a server using RPC. A malformed request to the host running the RPCSS service may result in a buffer overflow condition that will present the attacker with the opportunity to execute arbitrary code with the privileges of the local system account. Alternatively the attacker could also cause the RPC service to stop answering RPC requests and thus cause a Denial of Service condition to occur.</p>
Affected Systems	<p>Windows NT 4.0 Workstation and Server</p> <p>Windows NT 4.0 Terminal Server Edition</p> <p>Windows 2000</p> <p>Windows XP</p>

SID:2251

deleted.rules:

```
# alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg:"DELETED NETBIOS DCERPC Remote Activation bind attempt";
flow:to_server,established;
content:"|05|"; depth:1;
content:"|0B|"; within:1; distance:1; byte_test:1,&,1,0,relative;
content:"|B8|J|9F|M|1C|}|CF 11 86 1E 00| |AF|n|7C|W";
within:16; distance:29;
tag:session,5,packets;
reference:bugtraq,8234; reference:bugtraq,8458; reference:cve,2003-0528;
reference:cve,2003-0605; reference:cve,2003-0715; reference:nessus,11798;
reference:nessus,11835; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS03-039;
classtype:attempted-admin;
sid:2251; rev:18;)
```

Signature désormais désactivée

SID:2252

netbios.rules:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
```

```
(msg:"NETBIOS SMB-DS DCERPC Remote Activation bind attempt";
```

```
flow:to_server,established;
```

```
content:"|FF|SMB%"; depth:5; offset:4; nocase;
```

```
content:"&|00|"; within:2; distance:56;
```

```
content:"|5C 00|P|00|||00|P|00|E|00 5C 00|"; within:12; distance:5; nocase;
```

```
content:"|05|"; within:1;
```

```
content:"|0B|"; within:1; distance:1; byte_test:1,&,1,0,relative;
```

```
content:"|B8|J|9F|M|1C|}|CF 11 86 1E 00| |AF|n|7C|W"; within:16;
```

```
distance:29;
```

```
tag:session,5,packets;
```

```
metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, service netbios-ssn;
```

```
reference:bugtraq,8234; reference:bugtraq,8458; reference:cve,2003-0528;
```

```
reference:cve,2003-0605; reference:cve,2003-0715; reference:nessus,11798;
```

```
reference:nessus,11835; reference:url,technet.microsoft.com/en-us/security/bulletin/MS03-039;
```

```
classtype:attempted-admin;
```

```
sid:2252; rev:18;)
```

Outils complémentaires

- Oinkmaster
 - Récupération automatique des signatures
 - Barnyard
 - Insertion des alertes dans une base de données
 - Modèle de données
 - Efficacité
 - Consoles de visualisation
 - Principale valeur ajoutée des offres commerciales
 - Plusieurs générations
 - Exemples
 - ...
 - Sguil+Squert
 - Snorby
 - ...
- <http://manual.snort.org/>

Plus récemment...

- Vulnérabilité CVE-2012-4969 du 18/09/2012
 - Premiers détails le 14/09/2012
 - <http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/>
 - CERTA-2012-ALE-006-002 (en français)
- Identifiée sur des intrusions réelles
- Exécution arbitraire de code à distance
 - via un serveur Web malveillant
 - IE 6 à 9
 - Correctif Microsoft provisoire 2757760 du 19/09
 - « *0-day* »
- Snort
 - SID 24210
 - SID 24212
- Metasploit PoC (17/09/2012)
- ClamAV JS.Exploit.CVE_2012_4969
- Symantec : Bloodhound.Exploit.474/475,
Trojan.Dropper, Backdoor.Darkmoon

Fonctionnement

- « use after free »
- Metasploit
 - `ie_execcommand`

```
<body>
  <SCRIPT>
    var times = 0;
    var jifud = new Array();
    while(times < 100) {
      jifud[times] = window.document.createElement("img");
      jifud[times]["src"] = "a";
      times++;
    }
  </SCRIPT>
  x<embed src=Moh2010.swf width=10 height=10></embed>x
</body>
```

```
function SubtleArr() {
  document.execCommand("selectAll");
};

function TestArray() {
  if(f == 1)
  {
    document.write("L");
  }
  var L = 0;
  while(L < 99) {
    parent.jifud[L].src = "YMjf\u0c08\u0c0cKDogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuUFGGBSIPPPUDFJKSOQJGH"; ++L;
  }
}
```

```
</script>
<body onload='SubtleArr();'onselect='TestArray()'
```


Zoom (1/2)

```
<body>

  <SCRIPT>
    var times = 0;
    var jifud = new Array();
    while(times < 100) {
      jifud[times] = window.document.createElement("img");
      jifud[times]["src"] = "a";
      times++;
    }
  </SCRIPT>
  x<embed src=Moh2010.swf width=10 height=10></embed>x
</body>
```

Zoom (2/2)

```
function SubtleArr() {
    document.execCommand("selectAll");
};

function TestArray() {
    if(f == 1)
    {
        document.write("L");
    }
    var L = 0;
    while(L < 99) {
        parent.jifud[L].src = "YMjf\u0c08\u0c0cKDogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuU";
    }
}
```

```
</script>
```

```
<body onload='SubtleArr();'onselect='TestArray() '>
```

SID:24210

browser-ie.rules:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"BROWSER-IE Microsoft execCommand use-after-free attempt";
flow:to_client,established; file_data;
content:"execCommand(|22|selectAll|22|)"; fast_pattern:only;
content:"onload="; nocase;
content:"onselect="; within:50; nocase;
pcre:"/body[^\>]*?onload[^\>]*?onselect/i";
metadata:policy balanced-ips drop, policy security-ips drop, service http;
reference:url,labs.alienvault.com/labs/index.php/2012/new-internet-explorer-
zero-day-being-exploited-in-the-wild/;
classtype:attempted-user;
sid:24210; rev:2;)
```

Disponible depuis le 18/10/2012

SID:24212

browser-ie.rules:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"BROWSER-IE Microsoft execCommand use-after-free attempt";
flow:to_client,established; file_data;
content:"selectAll"; fast_pattern:only;
content:"document.write"; nocase;
content:"onselect="; nocase;
content:"execCommand";
pcre:"/execCommand\x28\s*?[\x22\x27]selectAll[\x22\x27]\s*?\x29/i";
metadata:policy balanced-ips drop, policy security-ips drop, service http;
reference:url,labs.alienvault.com/labs/index.php/2012/new-internet-explorer-
zero-day-being-exploited-in-the-wild/;
classtype:attempted-user;
sid:24212; rev:1;)
```

2003 & 2012 : Cuvées spéciales ?

- Nope
 - CVE-2013-3893 (publ. 18/09/2013)
 - Exécution arbitraire de code à distance
 - IE 6 à 11
 - CVE-2013-3907 (publ. 06/11/2013)
 - Exécution arbitraire de code à distance via une image TIFF spécialement conçue
 - Office 2003&2007&2010, Vista & Server 2008, +
 - Correctif (à la date d'actualisation du cours)
 - Désactiver le rendu graphique des images TIFF
 - :o)
- Pistes de réflexions - Enseignements
 - Retirer les images du cours ?
 - Former les nouvelles générations aux *emotes* à l'ancienne ;-)
 - Promouvoir la sécurité du mode texte
 - D'autres idées ?

Mais M'sieur, on est en 2014 !

- 04/11/2014, 11:52
 - okay, vous allez voir !
- www.cert.org : Oops !
 - NB : Java Coding Guidelines Available Free Online
- www.auscert.org.au
 - Drupal 7, ESB-2014-1995 : Automated remote arbitrary code/commands on Drupal <7.32 web sites started within hours of announcement.
 - « *You should proceed under the assumption that every Drupal 7 website was compromised unless updated or patched before Oct 15th, 11pm UTC, that is 7 hours after the announcement.* »
 - ESB-2014.1883 : Cisco IronPort Administrator compromise
 - ASB-2014.0121 : Oracle Products, multiple vulnerabilities
 - ASB-2014.0120 : Mozilla Firefox & co., multiple vulnerabilities

CVE-ID Syntax Change

Old Syntax

CVE-YYYY-NNNN

4 fixed digits, supports a maximum of 9,999 unique identifiers per year.

Fixed 4-Digit Examples

CVE-1999-0067

CVE-2005-4873

CVE-2012-0158

New Syntax

CVE-YYYY-NNNN...N

4-digit minimum and no maximum, provides for additional capacity each year when needed.

Arbitrary Digits Examples

CVE-2014-0001

CVE-2014-12345

CVE-2014-7654321

YYYY indicates year the ID is issued to a CVE Numbering Authority (CNA) or published.

Implementation date: January 1, 2014

Source: <http://cve.mitre.org>

Ready for
the future



Yara rule

- www.yara-project.org
- Description de programmes malveillants
 - Motifs textuels ou binaires
 - Combinaison des motifs

```
rule Internet_Explorer_8_0day
{
  meta:
    author = "Jaime Blasco"
    version = "v0.1"
    ref0 =
"http://dev.metasploit.com/redmine/projects/framework/repository/revisions/aac
41e91fd38f99238971892d61ead4cfbedabb4/entry/modules/exploits/windows/browser/i
e_execcommand_uaf.rb"

  strings:
    $s1 =
"YMjff\u0008\u000cKDogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuUFGGBSIPPPUDFJKSOQJGH"
    $s2 = "document.execCommand(\"selectAll\")"

  condition:
    all of them
}
```


Autres exemples (yara)

```
rule EntryPointExample2
{
  strings:
    $a = { 9C 50 66 A1 ?? ?? ?? 00 66 A9 ?? ?? 58 0F 85 }
  condition:
    $a in (entrypoint..entrypoint + 10)
}
```

```
rule OfExample3
{
  strings:
    $foo1 = "foo1"
    $foo2 = "foo2"
    $bar1 = "bar1"
    $bar2 = "bar2"
  condition:
    3 of ($foo*, $bar1, $bar2)
}
```

```
rule InExample
{
  strings:
    $a = "dummy1"
    $b = "dummy2"
  condition:
    $a in (0..100) and $b in (100..filesize)
}
```

YARA User's Manual, v1.6, Victor M. Álvarez

Remarques

- La CVE-2012-4969 est consécutive à une autre découverte
 - CVE-2012-4681
 - Oracle Java SE7 0-day
 - Diffusion publique le 26/08/2012
 - Metasploit : [java_jre17_exec.rb](#)
- Ecart entre CVE-2003-0528 et CVE-2012-4969
 - 9 ans
 - autre chose ?

Règles de détection d'anomalie

- En-tête PDF non-standard ou code d'identification aberrant
 - SID 16354
- SQL oversized cast/convert statement
 - SID 13791 /13987
- Suspicious .cn/.ru query
 - SID 15167/15168
- *Obfuscated ActiveX object instantiation*
 - *SID 16573 / 16574*

SID:16354

file-pdf.rules:

```
# alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"FILE-PDF Adobe Reader start-of-file alternate header obfuscation";
flow:established,to_client; flowbits:isset,file.pdf; file_data;
content:"%!PS-Adobe-"; fast_pattern:only;
metadata:policy security-ips drop, service http, service imap, service pop3;
reference:url,www.adobe.com/devnet/acrobat/pdfs/pdf\_reference\_1-7.pdf;
classtype:misc-activity;
sid:16354; rev:11;)
```

SID:15167

indicator-compromise.rules:

```
# alert udp $HOME_NET any -> $HOME_NET 53
```

```
(msg:"INDICATOR-COMPROMISE Suspicious .cn dns query";
```

```
flow:to_server;
```

```
content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
```

```
content:"|02|cn|00|"; distance:0; pcre:"/[\\x05-\\x20]
```

```
[bcdfghjklmnpqrstvwxyz]{5,32}[^\\x00]*?\\x02cn\\x00/i";
```

```
metadata:policy security-ips drop, service dns;
```

```
classtype:trojan-activity;
```

```
sid:15167; rev:11;)
```

SID:13791

indicator-obfuscation.rules:

```
# alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"INDICATOR-OBFUSCATION oversized cast statement - possible
sql injection obfuscation";
flow:established,to_server;
content:"CAST|28|"; nocase; isdataat:250,relative;
content:"!"|29|"; within:250;
metadata:policy security-ips drop, service http;
reference:url,isc.sans.org/diary.html?storyid=3823;
classtype:web-application-attack;
sid:13791; rev:4;)
```

sid:13987 *idem* pour CONVERT

SEL/**/ECT

- Les techniques d'évasion sont désormais très utilisées (*obfuscation*)
- Exemples d'idées (pour l'injection SQL)
 - Commentaires et espaces
 - Fragmentation de la requête injectée
 - Pollution des paramètres HTTP
 - Commentaires (spécifiques : non terminés, spéciaux)
 - Emplacement non examiné par les sondes
- Les sondes doivent en tenir compte

- Rq : Les techniques de chiffrement/signature de code sont aussi très développées (chez les attaquants)

```
0 div 1 union#foo*/*bar  
select#foo  
1,2,current_user
```

devient

```
0 div 1 union select 1,2,current_user
```


Squid

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.6422	2007-03-19 23:05:14	63.26.198.32		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	64	gateway	2.6424	2007-03-19 23:13:28	203.193.56.133	45026	209.120.188.193	22	6	BLEEDING-EDGE Potential SSH Scan
RT	1	gateway	2.6489	2007-03-19 23:52:22	213.7.12.116		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	1	gateway	2.6496	2007-03-20 00:28:10	24.178.8.170		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.5980	2007-03-18 20:31:06	85.188.1.26	6667	209.120.188.193	58870	6	BLEEDING-EDGE POLICY IRC connection
RT	1	gateway	2.6298	2007-03-19 08:03:51	87.240.48.122	1173	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6380	2007-03-19 18:37:24	220.178.43.82	3064	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6387	2007-03-19 19:16:20	202.101.62.218	1030	209.120.188.193	1434	17	MS-SQL version overflow attempt

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	4.3	2007-03-01 02:49:52	202.188.160.53	45398	209.120.188.193	22	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.4	2007-03-01 05:35:33	211.147.250.20	6000	209.120.188.193	3128	6	PADS New Asset - www squid/2.5.STABLE6
RT	1	gateway	4.5	2007-03-03 03:40:46	82.96.96.3	38419	209.120.188.193	23	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.6	2007-03-08 15:13:20	162.18.202.88	40942	209.120.188.193	44	6	PADS New Asset - ssh OpenSSH 4.3 (Protocol 2.0)

Sid	Net	Hostname	Type	Last	Status
1	Ext_Net	gateway	pcap	2007-03-20 00:49:23	UP
2	Ext_Net	gateway	snort	2007-03-20 00:28:10	UP
3	Ext_Net	gateway	sancp	2007-03-19 01:59:34	UP
4	Ext_Net	gateway	pads	2007-03-08 15:13:20	UP

Update Interval (secs): 120 NOW

Show Packet Data
 Show Rule
 www.snort.org
nvd.nist.gov

alert udp \$EXTERNAL_NET any -> \$HOME_NET 1434 (msg:"MS-SQL version overflow attempt"; flowbits:isnotset,ms_sql_seen_dns; dsize:>100; content:"|04|"; depth:1; reference:bugtraq,5310; reference:cve,2002-0649; reference:nessus,10674; reference:url,www.microsoft.com/technet/security/bulletin/MS02-020.aspx; classification:activity; sid:2050; rev:0)

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
UDP	220.178.43.82	209.120.188.193	4	5	0	404	31898	0	0	115	13184
UDP	Source Port	Dest Port	Length		ChkSum						
	3064	1434	384		37652						
DATA	<pre> 04 01 DC C9 B0 42 EB 0E 01 01 01 01 01 01 01 70 AE 42 01 70 AE 42 90 90 90 90 90 90 90 68 DC C9 B0 42 B8 01 01 01 01 31 C9 B1 18 50 E2 FD 35 01 01 01 05 50 89 E5 51 68 2E 64 6C 6C 68 65 6C 33 32 68 68 65 72 6E 51 68 6F 75 6E 74 68 69 63 6B 43 68 47 65 74 54 66 B9 6C 6C 51 68 33 32 2E 64 68 77 73 32 5F 66 B9 65 74 51 68 73 6F 63 6B 66 B9 74 6F 51 68 73 65 6E 64 BE 18 10 AE 42 8D 45 </pre>										

Search Packet Payload Hex Text NoCase

SUMMARY SIGNATURES IP MAP QUERY

< 2010 January February March April May June July August September October November December 2012 >
 Mon1 Tue02 Wed03 Thu04 Fri05 Sat06 Sun07 Mon08 Tue09 Wed10 Thu11 Fri12 Sat13 Sun14 Mon15 Tue16 Wed17 **Thu18** Sun19 Sat20 Sun21 Mon22 Tue23 Wed24 Thu25 Fri26 Sat27 Sun28 Mon29 Tue30 Wed31

Detail Lines: 10 Report Period: Thursday Aug 18, 2011

Brief



Event Distribution by Sensor

Network	Hostname	Agent Type	Last Event	Sig	Src	Dst	Count	% of Total
Toll	nssc-toll	snort	09:18:15	60	191	229	14549	94.66%
Campus	dnsbh-01	snort	09:18:07	8	40	3	821	5.34%
OLL	oll-01	snort	-	0	0	0	0	0

< 1 min < 5 min < 30 min > 30 min

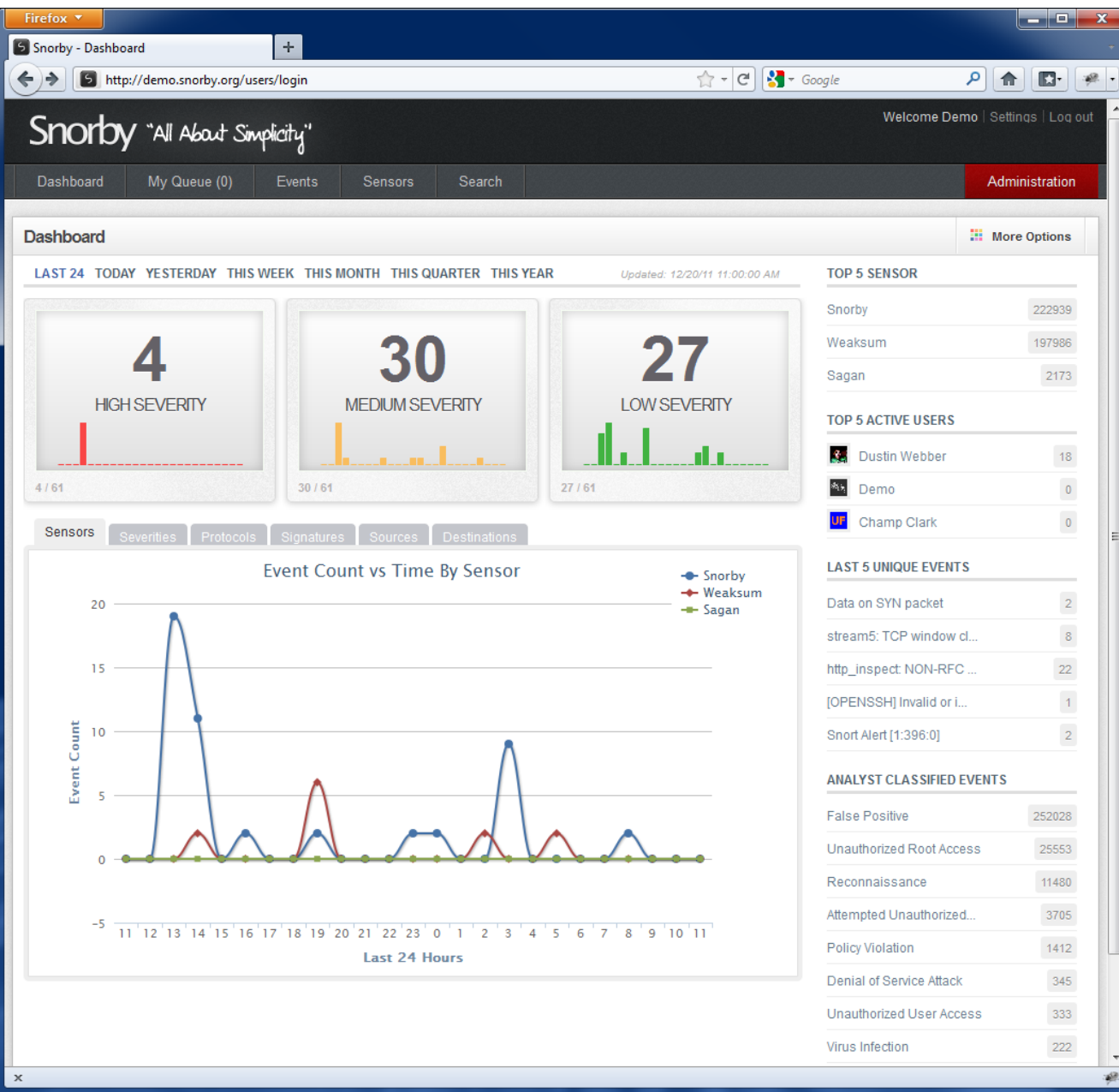
Event Distribution by Category

#	Category	Last Event	Sig	Src	Dst	Count	% of Total
UN	Unclassified	09:17:21	15	17	22	6431	41.84%
C1	Unauthorized Admin Access	-	0	0	0	0	0
C2	Unauthorized User Access	-	0	0	0	0	0
C3	Attempted Unauthorized Access	-	0	0	0	0	0
C4	Denial of Service Attack	-	0	0	0	0	0
C5	Policy Violation	09:15:53	28	100	160	2069	13.46%
C6	Reconnaissance	09:18:15	6	5	8	5794	37.7%
C7	Malware	09:17:46	15	110	64	1076	7%
ES	Escalated Event	-	0	0	0	0	0
NA	Expired Event	-	0	0	0	0	0

Top Signatures

Signature	ID	Last Event	Src	Dst	Count	% of Total
ssh: Protocol mismatch	4	09:17:21	2	5	6397	41.62%
ET SCAN Potential SSH Scan	2001219	09:18:14	3	7	4088	26.6%
INAPPROPRIATE Xhamster	2010111909	09:04:38	2	50	856	5.57%
ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool	2006435	09:18:10	1	4	685	4.46%
ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!	2006546	09:18:15	1	4	684	4.45%
MALWARE Blackhole Access (GET)	2011042801	09:13:49	38	1	472	3.07%

Squert



Console(s) de gestion

Snorby

Traitement et qualification des alertes

The screenshot shows the Snorby web interface in a Firefox browser. The page title is "Snorby - High Severity Events". The URL is [http://demo.snorby.org/results?search\[severity\]=1&search\[time_end\]=1324397928&search\[time_start\]=1](http://demo.snorby.org/results?search[severity]=1&search[time_end]=1324397928&search[time_start]=1). The interface includes a navigation menu with "Administration" highlighted in red. The main content area displays "High Severity Events" with 4 events found. A table lists the events, and a tooltip points to the "Event Signature" column of the third row, stating "Demo classified event as Attempted Unauthorized Access".

<input type="checkbox"/>	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
<input type="checkbox"/>	★ 1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011
<input type="checkbox"/>	★ 1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011
<input type="checkbox"/>	★ 1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011
<input type="checkbox"/>	★ 1	Snorby	CA 208.87.23.173	US 173.255.236.165	SHELLCODE x86 inc ebx NOOP	12/19/2011

Snorby 2.3.11 - <http://www.snorby.org> © 2011 Dustin Willis Webber

Prewikka

Prelude management

admin on Tuesday December 20 20 1 [logout](#)

Events

Agents

Users

About

Alerts Heartbeats Filters

Classification	Source	Target	Sensor	Time	
2 x User authentication via su successful (succeeded)	user: 0	user: process: su (9548)	PAM	15:17:48 - 15:17:45	<input type="checkbox"/>
User login successful (succeeded)	.46.50:54647/tcp	user: process: sshd (9536)	sshd	15:17:40	<input type="checkbox"/>
34 x DNS SPOOF query response with TTL of 1 min. and no authority	.9.30:53/udp	.7.49:65095/udp	snort ()	15:17:17 - 14:19:13	<input type="checkbox"/>
6 x Server recognition (failed)	.147.35:tcp	process: sshd (9528)	sshd	15:16:07 - 14:21:37	<input type="checkbox"/>
18 x VIRUS OUTBOUND bad file attachment	.20.12:57056/tcp	.0.10:25/tcp	snort ()	15:10:52 - 15:08:49	<input type="checkbox"/>
4 x Server recognition (failed)	.145.201:tcp	process: sshd (9496)	sshd ()	15:09:21 - 14:22:48	<input type="checkbox"/>
2 x WEB-PHP Pajax arbitrary command execution attempt	.15.200:35658/tcp	.0.100:8080/tcp	snort ()	14:58:56 - 14:58:26	<input type="checkbox"/>
WEB-CLIENT QuickTime Object ActiveX CLSID access	.100.40:8080/tcp	.53.100:53847/tcp	snort ()	14:58:16	<input type="checkbox"/>
1 x WEB-CLIENT Microsoft wmf metafile access	.53.100:52268/tcp	.00.40:8080/tcp	snort ()	14:44:57 - 14:27:26	<input type="checkbox"/>
1 x WEB-CLIENT Outlook EML access	.3.68:65373/tcp	.17.14:445/tcp	snort ()	14:41:09	<input type="checkbox"/>
NETBIOS SMB-DS Trans unicode Max Param/Count DOS attempt (vendor-specific:url, vendor-specific:url, vendor-specific:url, cve:2002-0724, bugtraqid:5556)	.5.20:8080/tcp	.00:58131/tcp	snort ()	14:36:01 - 14:36:00	<input type="checkbox"/>
5 x MISC Visio version number anomaly	.30:53/udp	.26:64876/udp	snort ()	14:35:50	<input type="checkbox"/>
DNS SPOOF query response with TTL of 1 min. and no authority					<input type="checkbox"/>

Delete

Filter:

Step: Hours

Tz:

Limit:

2011-12-20 14:18:11

2011-12-20 15:18:11

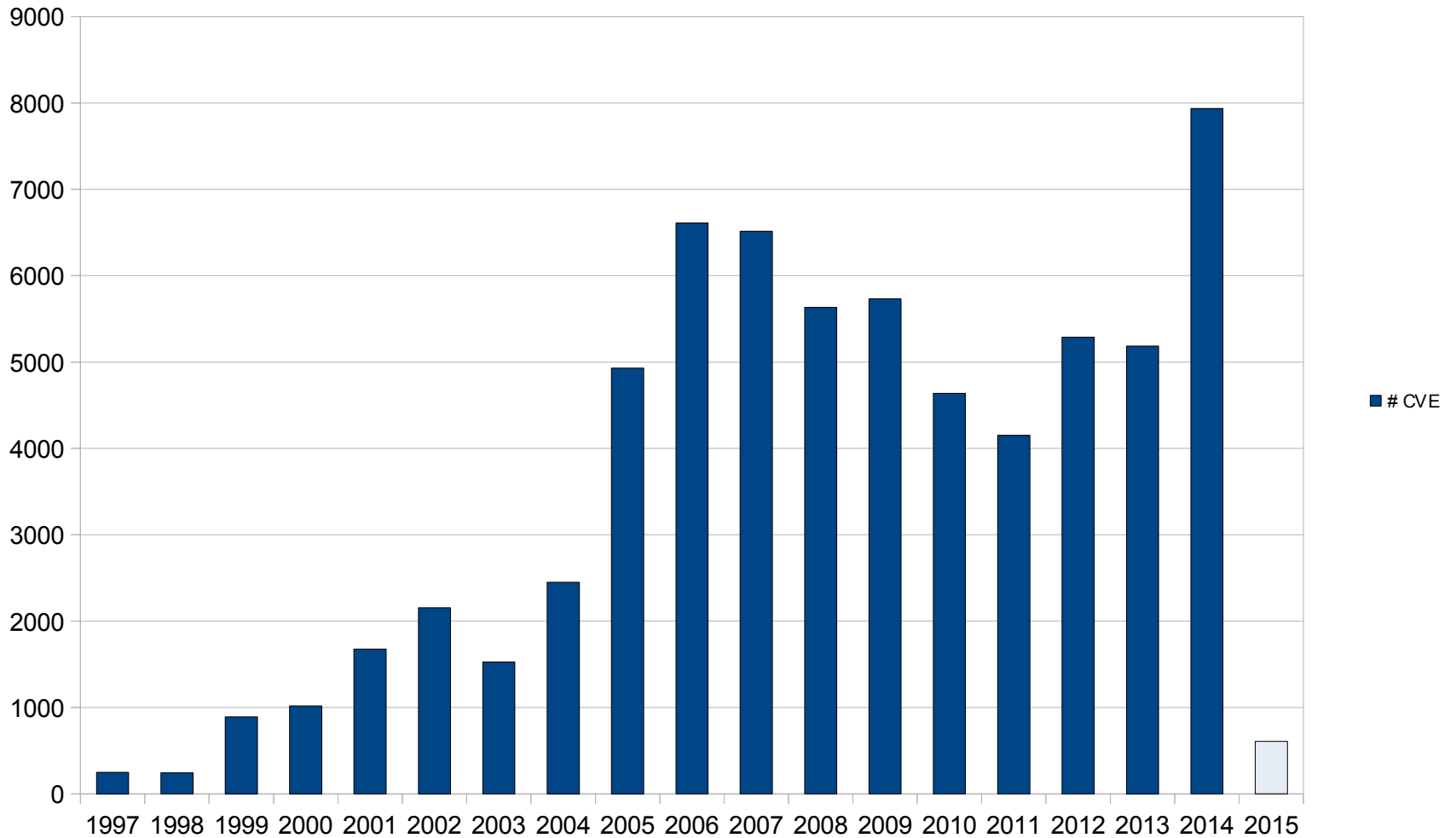
+01:00

1 ... 12 (total:12)

Limites actuelles de la détection d'intrusion

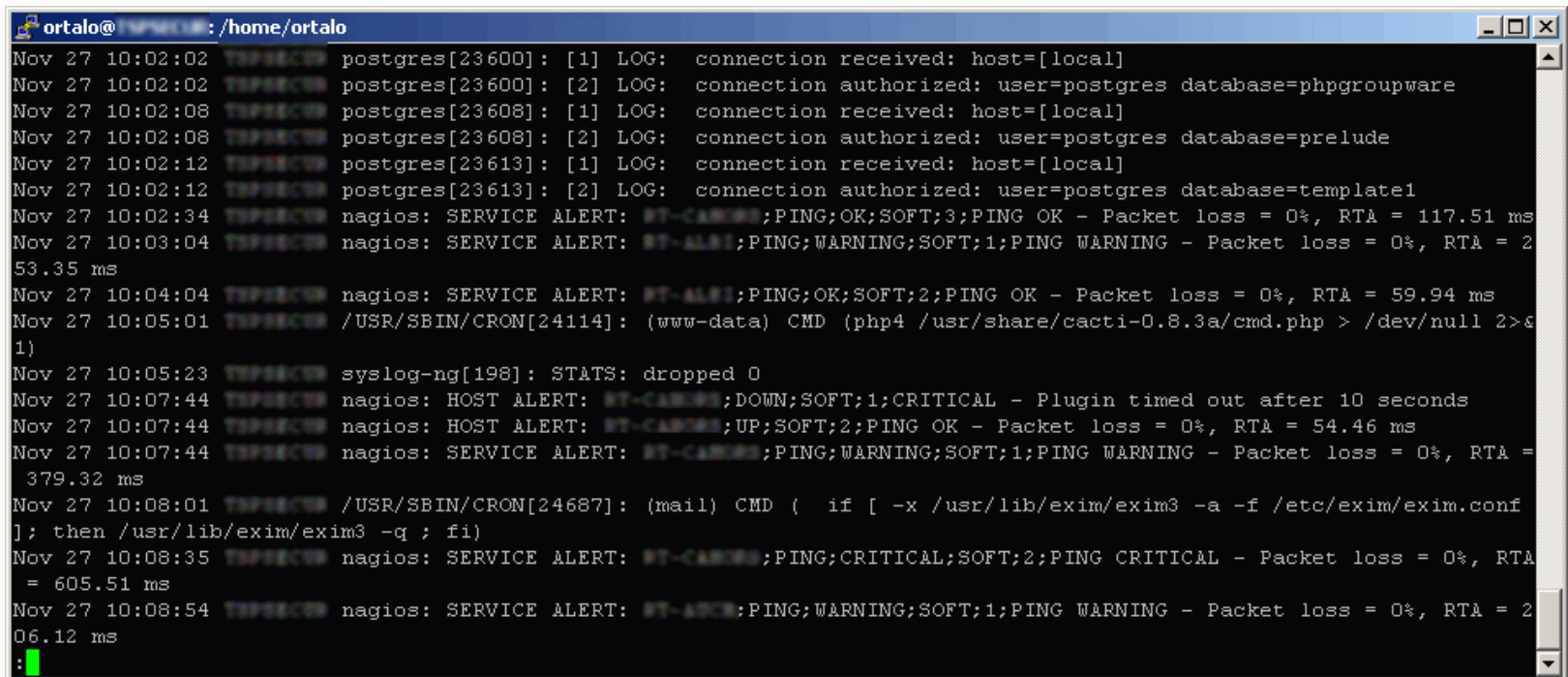
- Faible taux de détection
 - Faux négatifs
- Trop d'alertes
 - Fausses alertes : Faux positifs
 - Plusieurs milliers d'alertes générées en une semaine
- Le niveau de granularité d'une alerte est trop faible
 - Pas de vision globale
 - Difficile de détecter une attaque distribuée
- Difficile de détecter les attaques nouvelles
 - C'est un avantage des approches comportementales

Autre limite ?



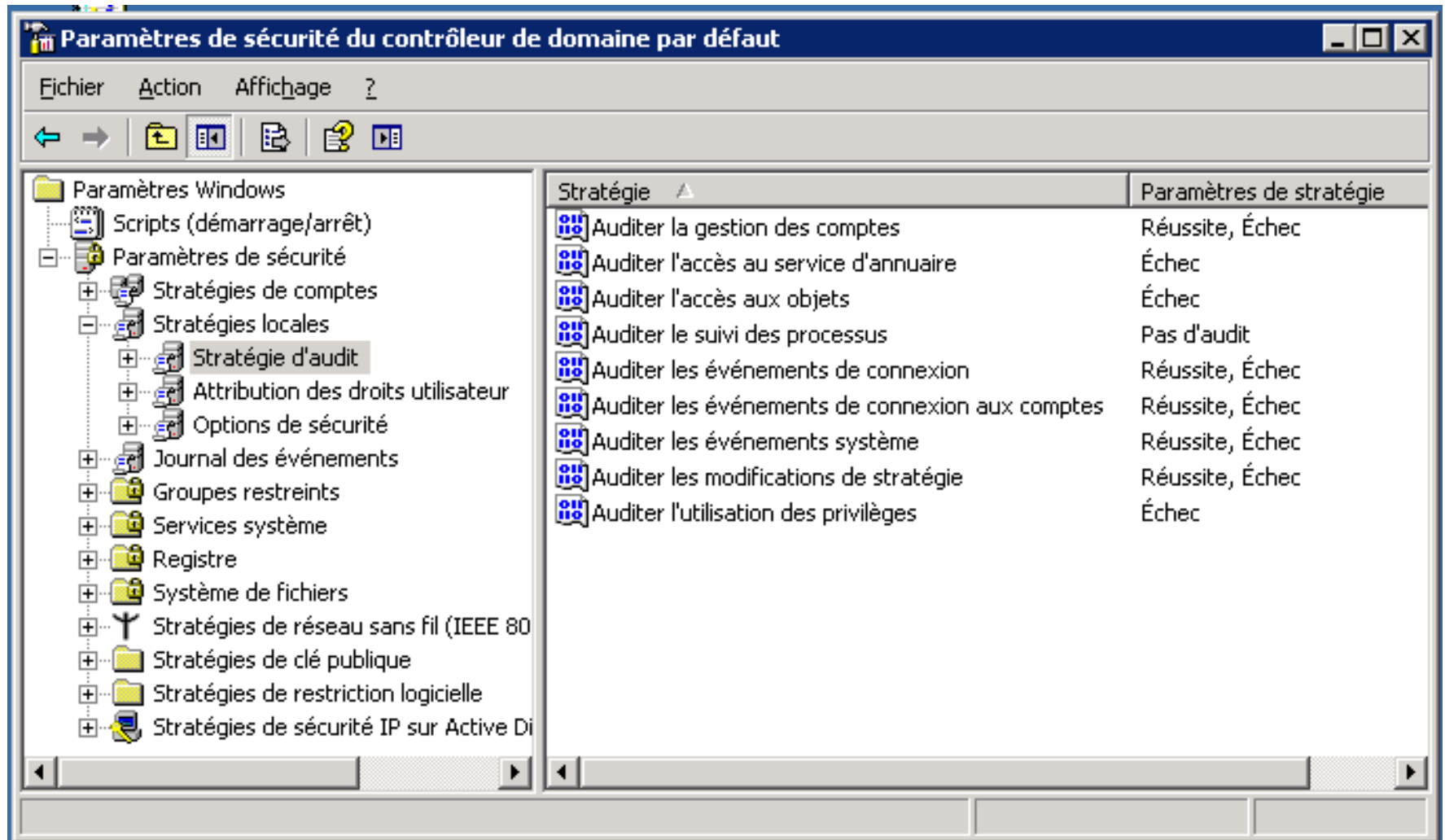
Centralisation des traces

- Solutions propriétaires
- Syslog
- CNIL



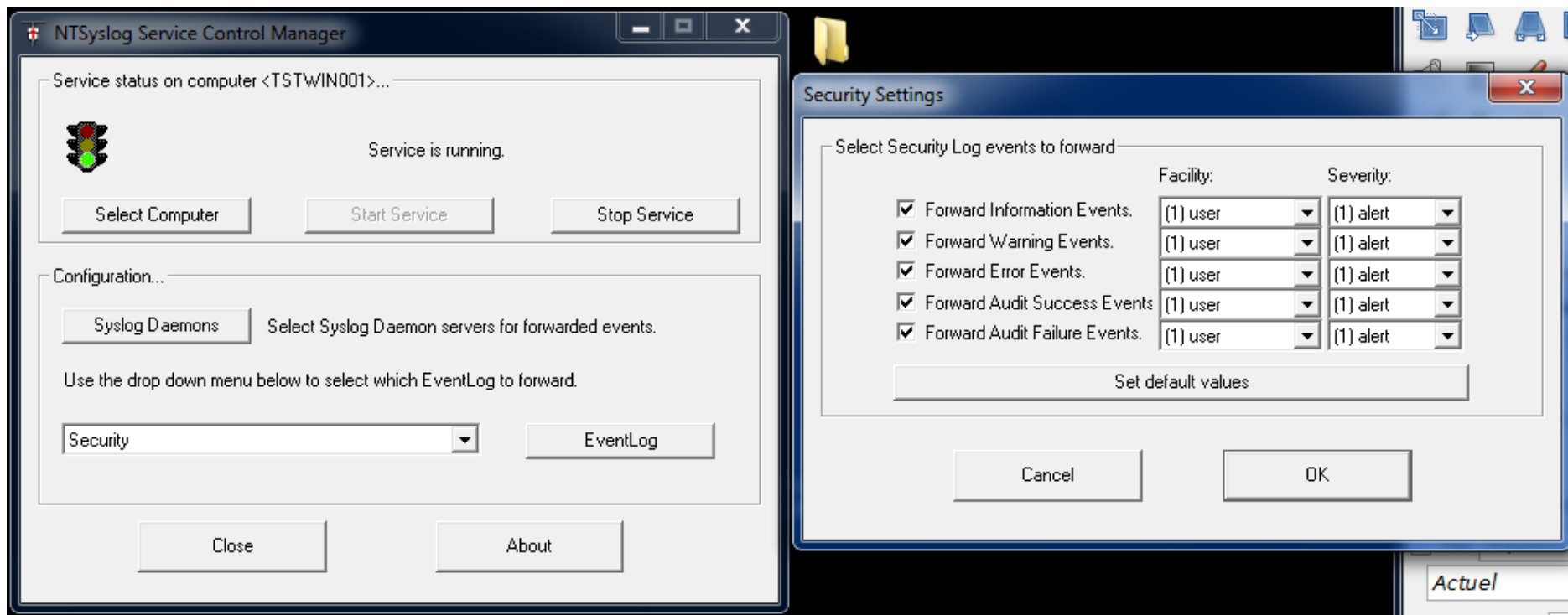
```
ortalo@ortalo: /home/ortalo
Nov 27 10:02:02 postgres[23600]: [1] LOG: connection received: host=[local]
Nov 27 10:02:02 postgres[23600]: [2] LOG: connection authorized: user=postgres database=phpgroupware
Nov 27 10:02:08 postgres[23608]: [1] LOG: connection received: host=[local]
Nov 27 10:02:08 postgres[23608]: [2] LOG: connection authorized: user=postgres database=prelude
Nov 27 10:02:12 postgres[23613]: [1] LOG: connection received: host=[local]
Nov 27 10:02:12 postgres[23613]: [2] LOG: connection authorized: user=postgres database=template1
Nov 27 10:02:34 nagios: SERVICE ALERT: BT-CARIBBE;PING;OK;SOFT;3;PING OK - Packet loss = 0%, RTA = 117.51 ms
Nov 27 10:03:04 nagios: SERVICE ALERT: BT-ALBA;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 253.35 ms
Nov 27 10:04:04 nagios: SERVICE ALERT: BT-ALBA;PING;OK;SOFT;2;PING OK - Packet loss = 0%, RTA = 59.94 ms
Nov 27 10:05:01 /USR/SBIN/CRON[24114]: (www-data) CMD (php4 /usr/share/cacti-0.8.3a/cmd.php > /dev/null 2>&1)
Nov 27 10:05:23 syslog-ng[198]: STATS: dropped 0
Nov 27 10:07:44 nagios: HOST ALERT: BT-CARIBBE;DOWN;SOFT;1;CRITICAL - Plugin timed out after 10 seconds
Nov 27 10:07:44 nagios: HOST ALERT: BT-CARIBBE;UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 54.46 ms
Nov 27 10:07:44 nagios: SERVICE ALERT: BT-CARIBBE;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 379.32 ms
Nov 27 10:08:01 /USR/SBIN/CRON[24687]: (mail) CMD ( if [ -x /usr/lib/exim/exim3 -a -f /etc/exim/exim.conf ]; then /usr/lib/exim/exim3 -q ; fi)
Nov 27 10:08:35 nagios: SERVICE ALERT: BT-CARIBBE;PING;CRITICAL;SOFT;2;PING CRITICAL - Packet loss = 0%, RTA = 605.51 ms
Nov 27 10:08:54 nagios: SERVICE ALERT: BT-ARCA;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 206.12 ms
:
```

Paramétrage d'un DC Windows

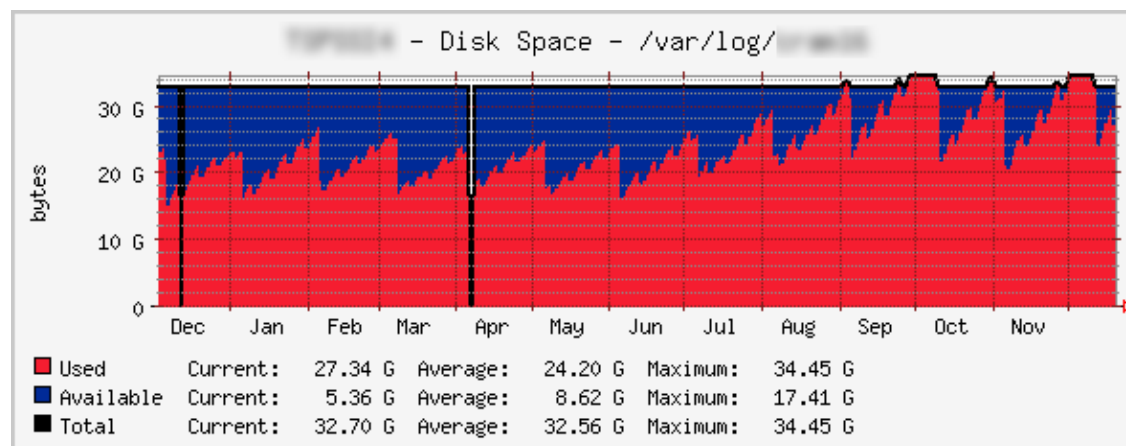
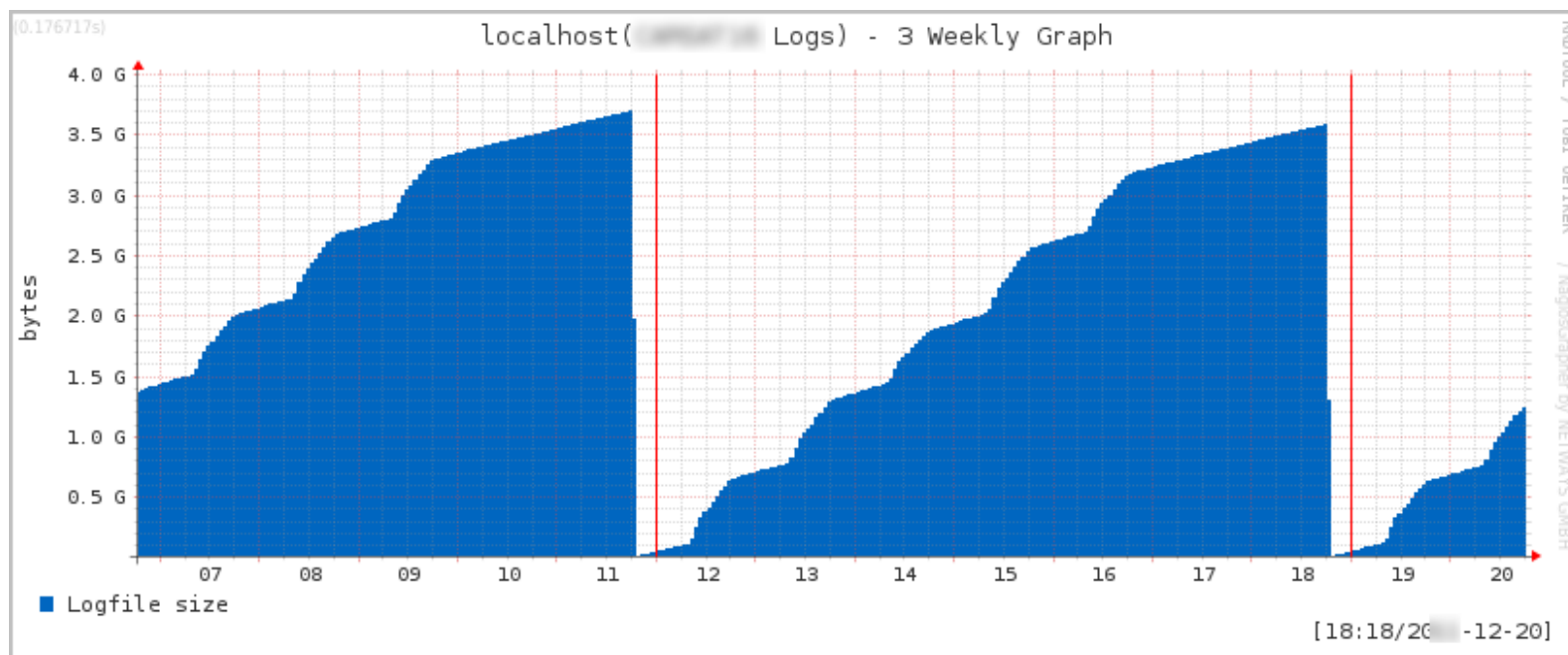


Déport de trace (simple)

Outil : NTsyslog



Éléments de volumétrie



Antivirus sur le poste (1)

The screenshot displays the Symantec Endpoint Protection user interface. At the top, the title bar reads "Symantec Endpoint Protection". The main area is titled "Etat" (Status) and features a large green banner with a white checkmark icon, stating "Votre ordinateur est protégé." (Your computer is protected.) and "Aucun problème détecté." (No problem detected.). Below this, a section titled "Technologies de protection" (Protection technologies) lists installed features. Two are shown: "Protection antivirus et antispyware" (Antivirus and antispyware protection) and "Protection proactive contre les menaces" (Proactive threat protection). Both are marked as "Activé" (Active) and include "Options" buttons. The interface also includes a left sidebar with navigation options like "Rechercher les menaces" (Search for threats) and "Afficher les journaux" (View logs), and a "LiveUpdate" button. The Symantec logo is visible in the bottom left corner.

Symantec Endpoint Protection

Aide et support

Etat

Rechercher les menaces

Changer les paramètres

Afficher la quarantaine

Afficher les journaux

LiveUpdate




Etat

Votre ordinateur est protégé.

Aucun problème détecté.

Technologies de protection

Les technologies de protection Symantec suivantes sont installées sur votre ordinateur :

	 Protection antivirus et antispyware Protège contre virus, chevaux de Troie, logiciels espions. Définitions : mardi 20 décembre 2011 r20	Activé	Options
	 Protection proactive contre les menaces Assure une protection immédiate contre les menaces inconnues. Définitions : mardi 20 décembre 2011 r5	Activé	Options

symantec.

Antivirus sur le poste (2)

The screenshot displays the Symantec Endpoint Protection user interface. At the top, the title bar reads "Symantec Endpoint Protection". The main heading is "Rechercher les menaces" (Search for threats), with an "Aide et support" (Help and support) button in the top right. On the left, a navigation menu includes "Etat" (Status), "Rechercher les menaces" (highlighted), "Changer les paramètres" (Change settings), "Afficher la quarantaine" (Show quarantine), "Afficher les journaux" (Show logs), and "LiveUpdate".

The main content area is divided into two columns for scan options:

- Active Scan:** "Analyser uniquement les zones les plus communément infectées." (Analyze only the most commonly infected areas). Duration: "1 a 2 minutes". Button: "Exécuter Active Scan".
- Analyse complète:** "Analyser l'ensemble de l'ordinateur." (Analyze the entire computer). Duration: "30 a 120 minutes". Button: "Exécuter une analyse complète".

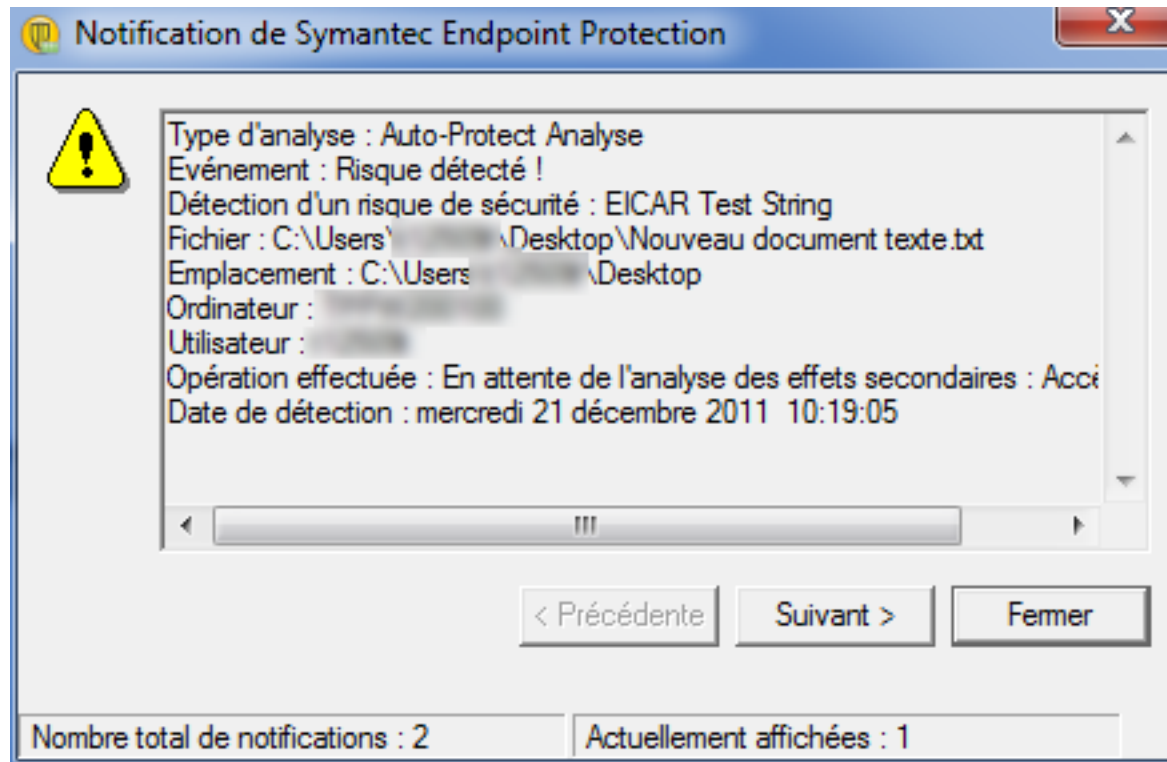
Below these options, the "Analyses" section states "Analyses configurées pour cet ordinateur." (Analyses configured for this computer) and includes a "Créer une analyse" (Create analysis) link.

A table lists the configured analyses:

Nom de l'analyse	Activé	Type	Moment de l'analyse	Dernière analyse
Analyse planifiée chaque semaine	Oui	Analyse com...	Hebdomadaire	lundi 19 décembre 2011 22.

The Symantec logo is visible in the bottom left corner of the interface.

Antivirus sur le poste (3)



Console Antivirus (1)

The screenshot shows the Symantec Endpoint Protection Manager console. The interface is in French and displays various security metrics and reports.

Console Symantec Endpoint Protection Manager

Symantec™ Endpoint Protection Manager Actualiser A propos de Aide Déconnexion

Etat de la sécurité [Préférences](#)
Etat de la sécurité - Bon [Infos supplém.](#)

Résumé des actions par nombre de détections

Opération	Virus	Risques de sécurité
Nettoyé	0	0
Suspect	0	0
Bloqué	0	0
Mis en quarantaine	0	0
Supprimé	0	0
Nouvellement infecté	0	0
Encore infecté	1	0

Risques par heure : 12 dernières heures
Afficher : Risques

Résumé de l'état

	Ordinateurs
Moteur antivirus arrêté	0
Auto-Protect arrêté	0
Protect contre intervent. désactiv	0
Redémarrage requis	1
Intégrité de l'hôte défaillante	0
Etat élément n'effectu. pas rappo.	0

Distribution des définitions de virus : 12 dernières heures
Afficher : Distribution des définitions de virus

Définitions	Ordinateurs
2011-12-20 rev. 020	725
2011-12-20 rev. 002	1
2011-12-19 rev. 020	3
2011-12-18 rev. 009	1
tous les autres	11

Security Response Dernière mise à jour : 21/12/2011 07:38:55

Men princip Dernier change. propa. : 09/10/2010 00:56:01

» Aucun article à afficher

Dernières menaces

» Aucun article à afficher

Il n'y a actuellement pas de menaces de catégorie 3 ou plus en circulation.

Symantec ThreatCon

- Alerte de sécurité
- Symantec
- Définitions
- Dernières menaces
- Security Focus

Level 1: Normal

Résumé des applications surveillées

	Occurrences
Détection d'application commerciale	0
Détect. proactive forcée menaces TruScan	0

Rapports sur les favoris [+](#)

- Principales sources d'attaques
- Corrélation des principaux risques
- Distrib. ds menaces protect TruScan

Administrateur

Aucune notification non acquittée dans les 24 dernières heures

Console Antivirus (3)

Téléchargements les plus récents de LiveUpdate

Affiche les téléchargements les plus récents de contenu LiveUpdate sur ce site. L'affichage n'affiche pas les téléchargements LiveUpdate sur les clients. Il n'affiche pas non plus les téléchargements des paquets d'installation de client.

Type de contenu	Révision	Moment du téléchargement
Catalogue de contenus de Symantec Endpoint Protection Manager 11.0	2011-05-19 rev. 701	21 septembre 2011 07:14:25 CEST
Définitions antivirus et contre les logiciels espions Win64 11.0 MicroDefs...	2011-12-20 rev. 020	21 décembre 2011 07:26:23 CET
Définitions antivirus et contre les logiciels espions Win32 11.0 MicroDefs...	2011-12-20 rev. 020	21 décembre 2011 07:39:04 CET
Decomposer Win32 et Win64 11.0	2008-02-17 rev. 000	24 septembre 2009 14:30:05 CEST
Moteur d'analyse proactive des menaces TruScan Win64 11.0	2008-08-20 rev. 001	24 septembre 2009 14:32:43 CEST
Données d'analyse proactive des menaces TruScan 11.0	2008-08-20 rev. 001	24 septembre 2009 14:32:34 CEST
Moteur d'analyse proactive des menaces TruScan Win32 11.0	2008-08-20 rev. 001	24 septembre 2009 14:32:48 CEST
Liste blanche d'analyse proactive des menaces TruScan Win32 11.0	2011-12-20 rev. 005	21 décembre 2011 07:46:23 CET
Liste des applications commerciales d'analyse proactive des menaces Tr...	2011-12-20 rev. 005	21 décembre 2011 07:47:53 CET
Moteur d'application commerciale d'analyse proactive des menaces TruS...	2008-09-29 rev. 016	24 septembre 2009 14:29:56 CEST
Liste blanche d'analyse proactive des menaces TruScan Win64 11.0	2011-12-20 rev. 005	21 décembre 2011 07:47:11 CET
Liste des applications commerciales d'analyse proactive des menaces Tr...	2011-12-20 rev. 005	21 décembre 2011 07:46:15 CET
Signatures de prévention d'intrusions Win32 11.0	2011-12-20 rev. 001	21 décembre 2011 07:20:54 CET
Signatures de prévention d'intrusions Win64 11.0	2011-12-20 rev. 001	21 décembre 2011 07:47:03 CET
Signatures de contrôle des transmissions 11.0	2010-12-01 rev. 096	3 décembre 2010 06:29:22 CET

Fermer

Console Antivirus (2)

The screenshot displays the Symantec Endpoint Protection Manager interface. The top navigation bar includes 'Actualiser', 'A propos de', 'Aide', and 'Déconnexion'. The left sidebar contains navigation options: 'Page démarrage', 'Contrôles', 'Rapports', 'Politiques', 'Clients', and 'Administrateur'. The main area is titled 'PC Standard' and shows a tree view of client groups with 'PC Standard' selected. Below the tree, a table lists the clients in this group, showing columns for 'Nom', 'Client d'ouverture de session', 'Adresse IP', 'Version de client', 'Dernier contrôle', and 'Redémarrage'. The table indicates that the group contains 35 clients, with the current view showing the first 25.

Nom	Client d'ouverture de session	Adresse IP	Version de client	Dernier contrôle	Redémarrage
			11.0.5002.333	20/12/11 16:59	Non
			11.0.5002.333	19/12/11 17:11	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	02/12/11 14:31	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	20/12/11 16:35	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	13/12/11 08:34	Non
			11.0.5002.333	16/12/11 16:59	Non
			11.0.5002.333	16/12/11 16:19	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	25/11/11 11:11	Non
			11.0.5002.333	13/12/11 15:35	Non
			11.0.5002.333	08/12/11 17:59	Non
			11.0.5002.333	20/12/11 16:39	Non
			11.0.5002.333	09/12/11 15:59	Non
			11.0.5002.333	21/12/11 10:28	Non
			11.0.5002.333	20/12/11 17:03	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	16/12/11 16:59	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	21/12/11 10:24	Non
			11.0.5002.333	21/12/11 10:32	Non
			11.0.5002.333	20/12/11 17:47	Non
			11.0.5002.333	21/12/11 10:24	Non
			11.0.5002.333	20/12/11 10:27	Non

Console Antivirus (3)

Symantec™ Endpoint Protection Manager [Actualiser](#) | [A propos de](#) | [Aide](#) | [Déconnexion](#)

Afficher les politiques

- Antivirus et antispyware
- Pare-feu
- Prévention d'intrusion
- Contrôle des applications et des ...
- LiveUpdate
- Exceptions centralisées
- Composants de politique ▲

Tâches

- Ajouter une politique antivirus et :
- Importer une politique antivirus et
- Rechercher des applications

Politiques antivirus et antispyware

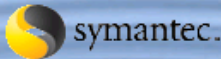
Nom	Description	Compte de l'utilisat...
Politique antivirus et antispyware	Politique recommandée pour la plupart des environnements, offrant ...	0
Politique antivirus et antispyware - Haut...	Politique haute sécurité, pouvant affecter les performances d'autres...	0
Politique antivirus et antispyware - Haut...	Politique offrant de meilleures performances mais une sécurité inféri...	0
Politique antivirus et antispyware Test s...	Politique Test	0
V1 - Politique antivirus et antispyware p...	Politique par défaut pour les serveurs	10
Sans scan planifiés - Politique antivirus ...	Politique sans scan	0
V2 - Politique antivirus et antispyware	Politique par défaut pour les clients standards	11
V2 - Serveurs Citrix - politique antivirus ...	Politique pour serveurs Citrix	1
V2 - Politique antivirus et antispyware - ...	idem politique livrée pour clients standards mais avec analyse planifi...	4
Test BM Exclusion	Test Exclusion	0

Les modifications récentes sont répertoriées ci-dessous :

Description	Heure	Administrateur
-------------	-------	----------------

Console Antivirus (3)

http://localhost:8014/ - Reporting - Nouveaux risques détectés dans le réseau - Windows Internet Explorer

Symantec Endpoint Protection 

Nouveaux risques détectés dans le réseau

20 Septembre 2011 11:00 PM à 21 Décembre 2011 11:59 PM Imprimer Enregistrer Fermer

15 entrées

Nom du risque Categorie / Type Découvert	Première occurrence Détecté par	Domaine Serveur Groupe	Ordinateur Utilisateur
▶ Infostealer 1 / Viral (Fichier) 08/12/1997	15/12/2011 08:07:15 Analyse Auto-Protect	Par défaut Ma société\PC Standard	
▶ Backdoor.Cycbot 1 / Viral (Fichier) 30/10/2010	15/12/2011 08:07:06 Analyse Auto-Protect	Par défaut Ma société\PC Standard	
▶ Trojan.Malscript 1 / Viral (Fichier) 27/10/2010	14/12/2011 11:23:31 Analyse Auto-Protect	Par défaut Ma société\PC Standard	
▶ Spyware.Netobserve Non spécifié / Logiciel espion (Fichier) Inconnue	06/12/2011 09:54:33 Analyse planifiée	Par défaut Ma société\PC Standard	
▶ Trojan.Gen.2 1 / Viral (Fichier) 20/08/2010	28/11/2011 09:03:30 Analyse Auto-Protect	Par défaut Ma société\PC Standard	
▶ CainAbel Non spécifié / Risque de sécurité (Fichier) Inconnue	23/11/2011 10:59:38 Analyse Auto-Protect	Par défaut Ma société\ajout fonctionnalites	
▶ Adware.InetAntiSpy Non spécifié / Logiciel de publicité (Fichier) Inconnue	17/11/2011 11:36:03 Analyse Auto-Protect	Par défaut Ma société\PC Standard	
▶ Bloodhound.Olexe 1 / Viral (Fichier) 20/11/2011	17/11/2011 09:31:38 Analyse Auto-Protect	Par défaut Ma société\PC Standard	

Signatures ClamAV

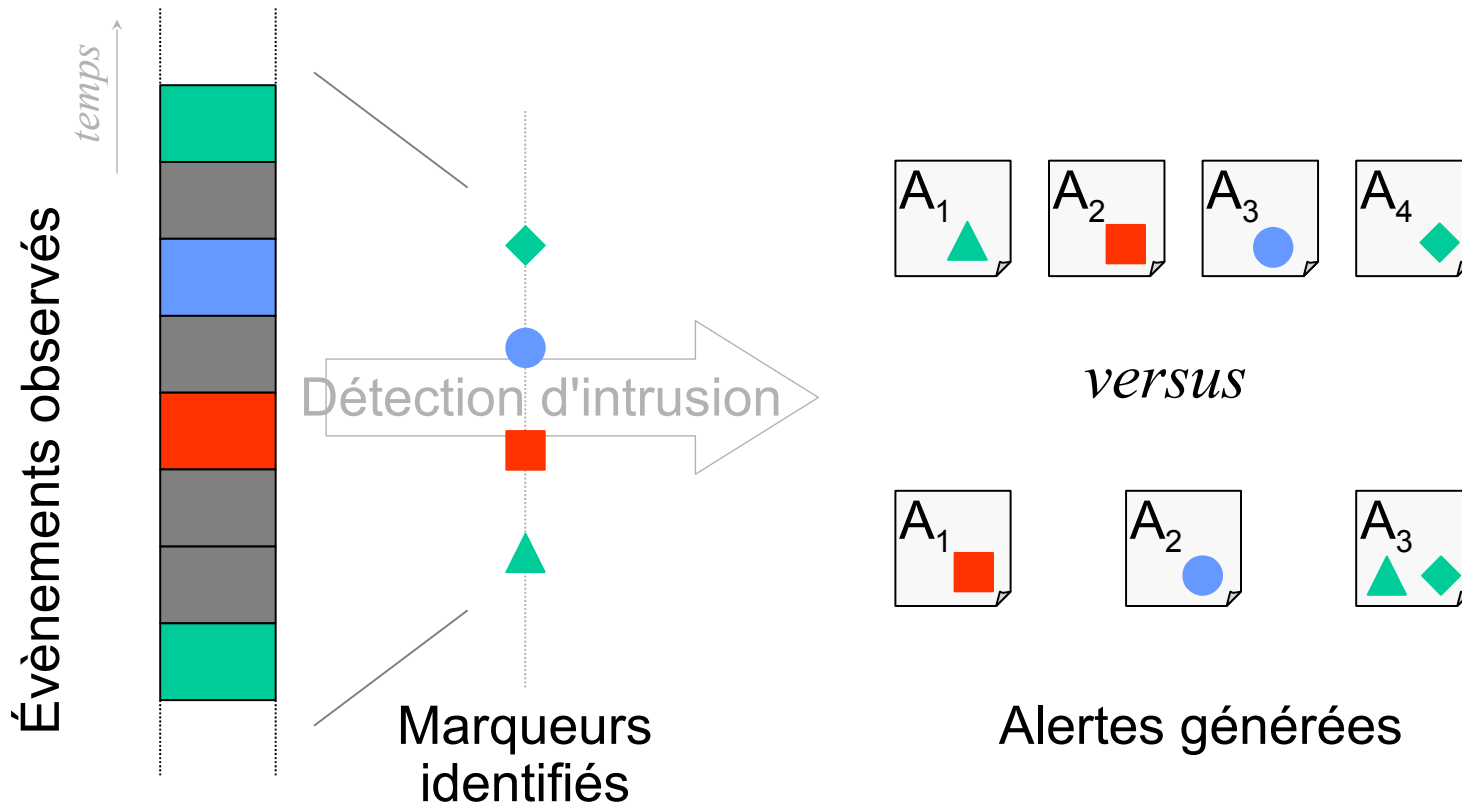
- Schématiquement
 - une empreinte (MD5, ...)
 - d'un (morceau) du fichier
 - (ou de ses méta-données : icône, etc.)

<http://www.clamav.net/doc/latest/signatures.pdf>

Outils complémentaires

- Analyse d'un flux réseau
 - Wireshark
- Contrôle de l'intégrité d'un système de fichiers
 - Outils disponibles
 - md5sum, sha1sum, *sha3sum* (2012+)
 - Samhain, AIDE
 - Problématiques de la famille « Tripwire »
 - Protection des empreintes de référence
 - Stockage externe ou hors ligne
 - Signature
 - Mise en oeuvre sur systèmes de fichiers réels
 - Fichiers spéciaux (/dev, etc.)
 - Traces
 - Binaires et mises à jour

Analyse multi-événements



Granularité trop fine

Exemple : alertes générées par Dragon



[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80

[**] [1:1002:2] WEB-IIS cmd.exe access [**]

07/20-13:59:33.969027	SID	1256
[**] [1:1256:2]	Message	WEB-IIS CodeRed v2 root.exe access
07/20-13:59:33.969027	Signature	alert tcp \$EXTERNAL_NET any -> \$HTTP_SERVERS \$HTTP_PORTS (msg:"WEB-IIS CodeRed v2 root.exe access"; flow:to_server,established; uricontent:"/root.exe"; nocase; classtype:web-application-attack; reference:url,www.cert.org/advisories/CA-2001-19.html; sid:1256; rev:7;)

07/20-13:59:33.969027 64.165.187.170:4582 -> 193.54.194.111:80

[**] [1:1288:2] WEB-FRONTPAGE /_vti_bin/ access [**]

07/20-13:59:34.434017 64.165.187.170:4587 -> 193.54.194.111:80

[**] [1:1002:2] WEB-IIS cmd.exe access [**]

07/20-13:59:34.817953 64.165.187.170:4593 -> 193.54.194.111:80

[**] [1:1002:2] WEB-IIS cmd.exe access [**]

07/20-13:59:35.219711 64.165.187.170:4601 -> 193.54.194.111:80

[**] [1:1002:2] WEB-IIS cmd.exe access [**]

07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80

07/20-13:59:35.607048	SID	1002
[**] [1:1002:2]	Message	WEB-IIS cmd.exe access
07/20-13:59:35.607048	Signature	alert tcp \$EXTERNAL_NET any -> \$HTTP_SERVERS \$HTTP_PORTS (msg:"WEB-IIS cmd.exe access"; flow:to_server,established; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:5;)

Granularité trop fine

Exemple : alertes générées par Dragon



```
[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]  
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:33.659882 64.165.187.170:4533 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:34.817953 64.165.187.170:4593 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:35.215711 64.165.187.170:4601 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
```

Attaque *Nimda* de 64.165.187.170
vers 193.54.194.111



Sémantique trop pauvre

Exemple : alertes générées par Dragon



```
[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]  
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:33.659882 64.165.187.170:4533 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:35.215711 64.165.187.170:4601 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80  
[**] [1:1002:2] WEB-IIS cmd.exe access [**]  
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
```

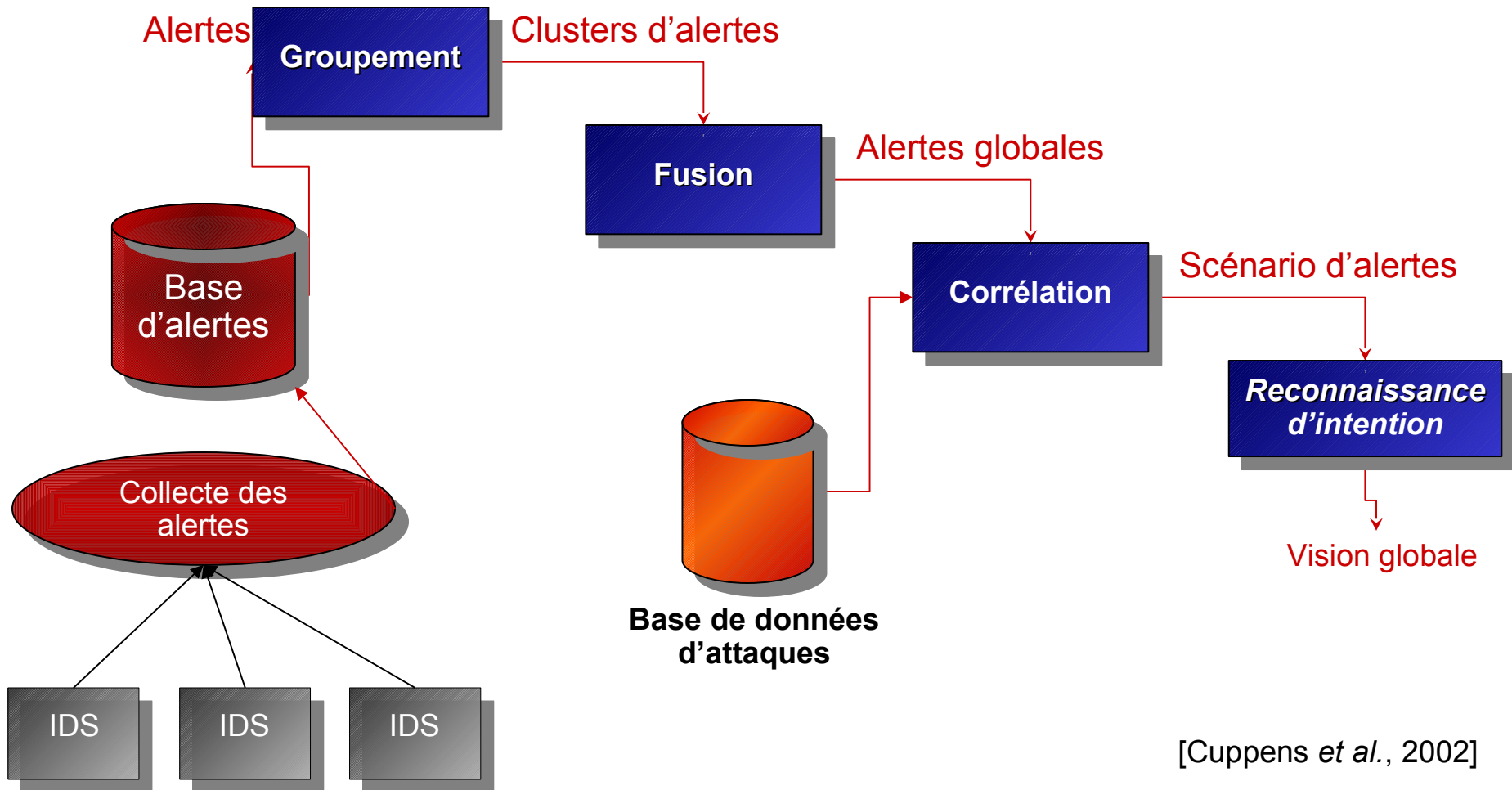
Attaque *Nimda* de 64.165.187.170
vers 193.54.194.111,
193.54.194.111 non-vulnérable



Corrélation d'alertes

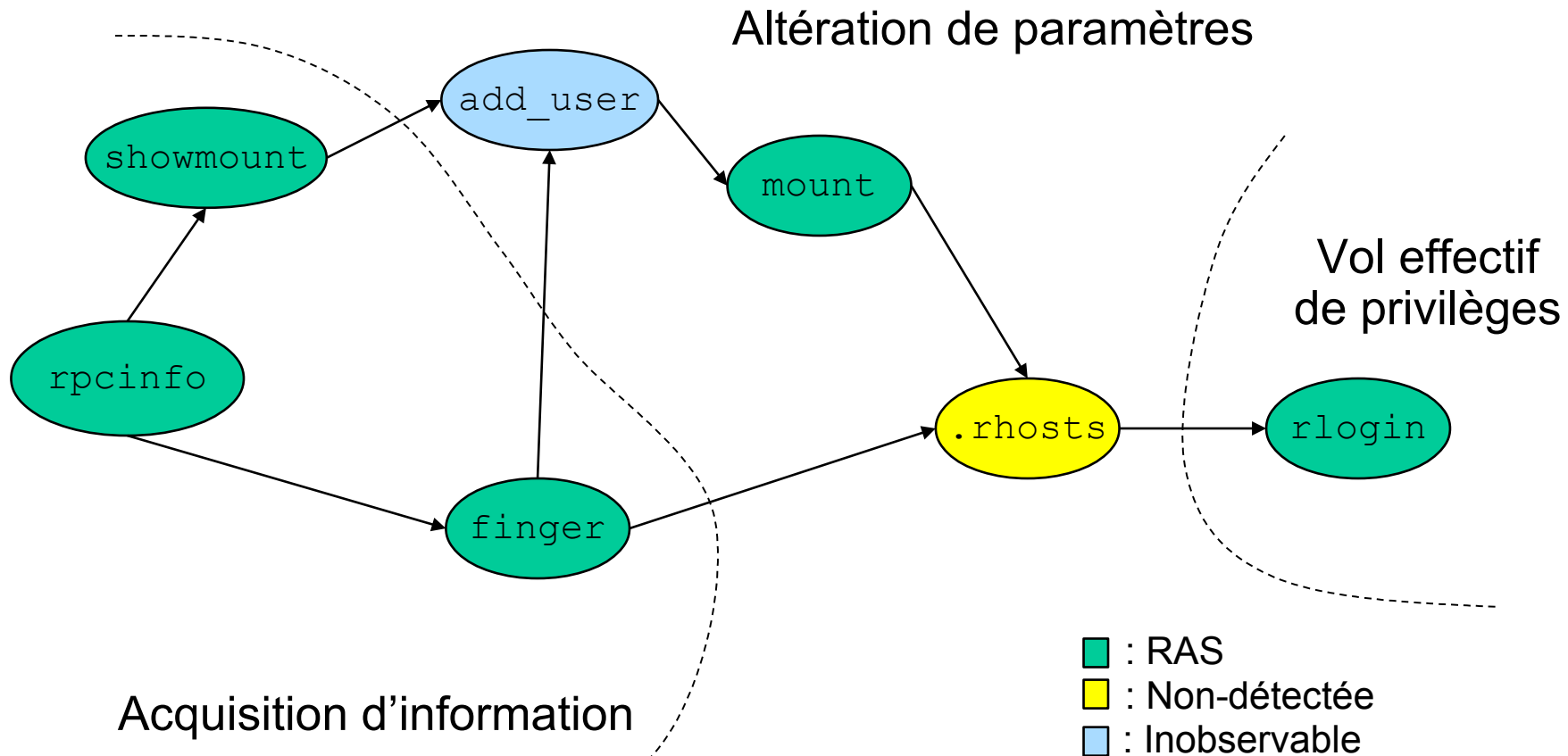
- Développement des méthodes utilisables pour la corrélation
- Prise en compte d'information de cartographie
- Intégration de notions de groupement puis de fusion dans des outils existants ?

Les étapes du diagnostic

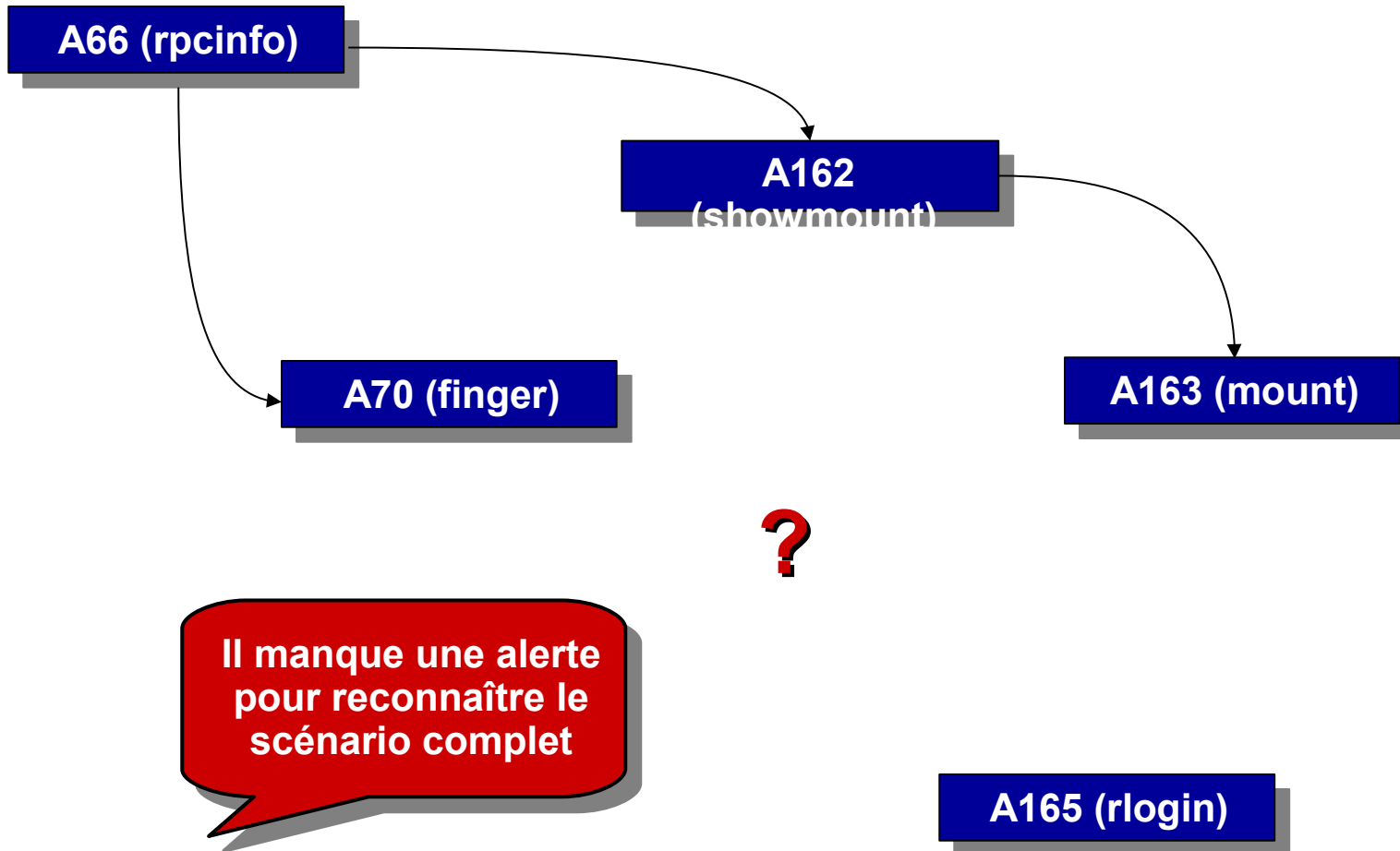


[Cuppens *et al.*, 2002]

Scénario non-linéaire (exemple)



Exemple de corrélation



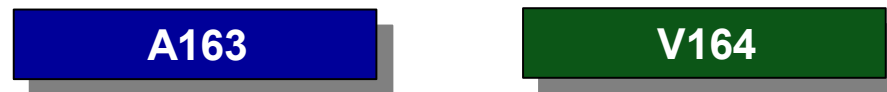
Génération d'hypothèse



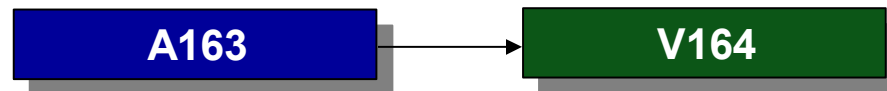
- ▶ On cherche une attaque appropriée



- ▶ Création d'une alerte en tant qu'instance de cette attaque



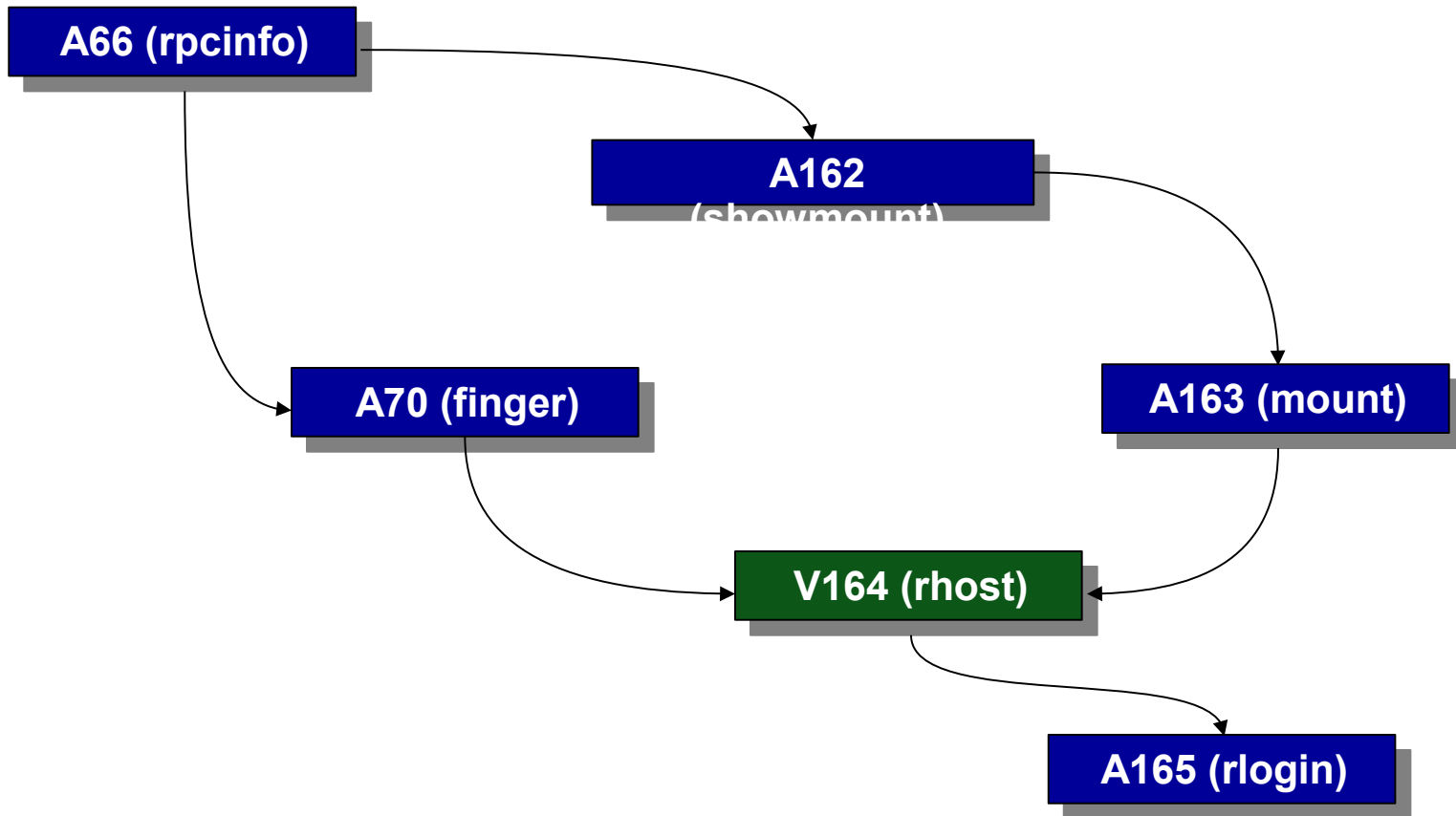
- ▶ Initialisation des champs de l'alerte grâce aux règles de corrélation



- ▶ Tentative de corrélation des deux dernières alertes



Résultat de la génération d'hypothèses



Plan (2/2)

- Protection utilisées dans la pratique
 - Protection réseau et *firewall*
 - Systèmes d'authentification
 - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
 - Détection d'intrusion
 - **Audit, tests d'intrusion**
 - Administration, exploitation et suivi de la sécurité
 - Observation et surveillance
- Protection des applications usuelles

Tests d'intrusion externes

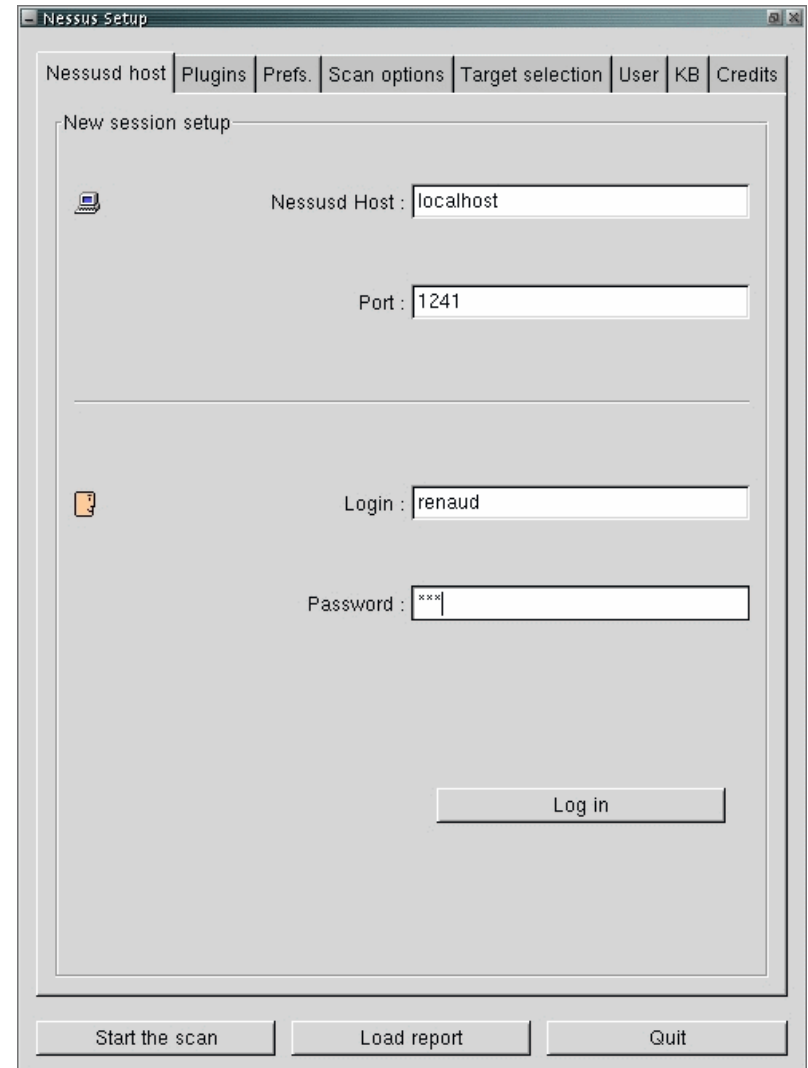
- Une prestation assez répandue
- Avantages
 - Indépendance des acteurs
 - Bien délimitée
- Inconvénients
 - Ponctuelle
 - Limitée au périmètre accessible (Internet, infrastructure sécurité)
 - Dé-corrélée de la politique de sécurité
- Similaire à une simulation d'attaque

Outils d'audit

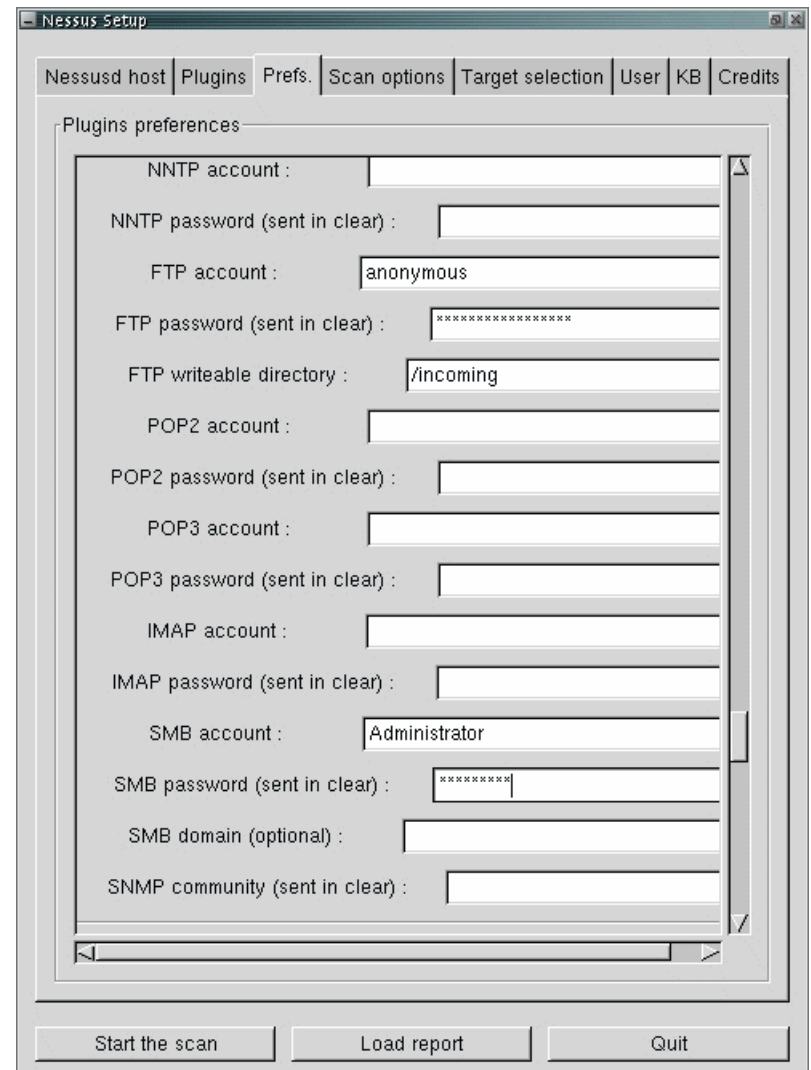
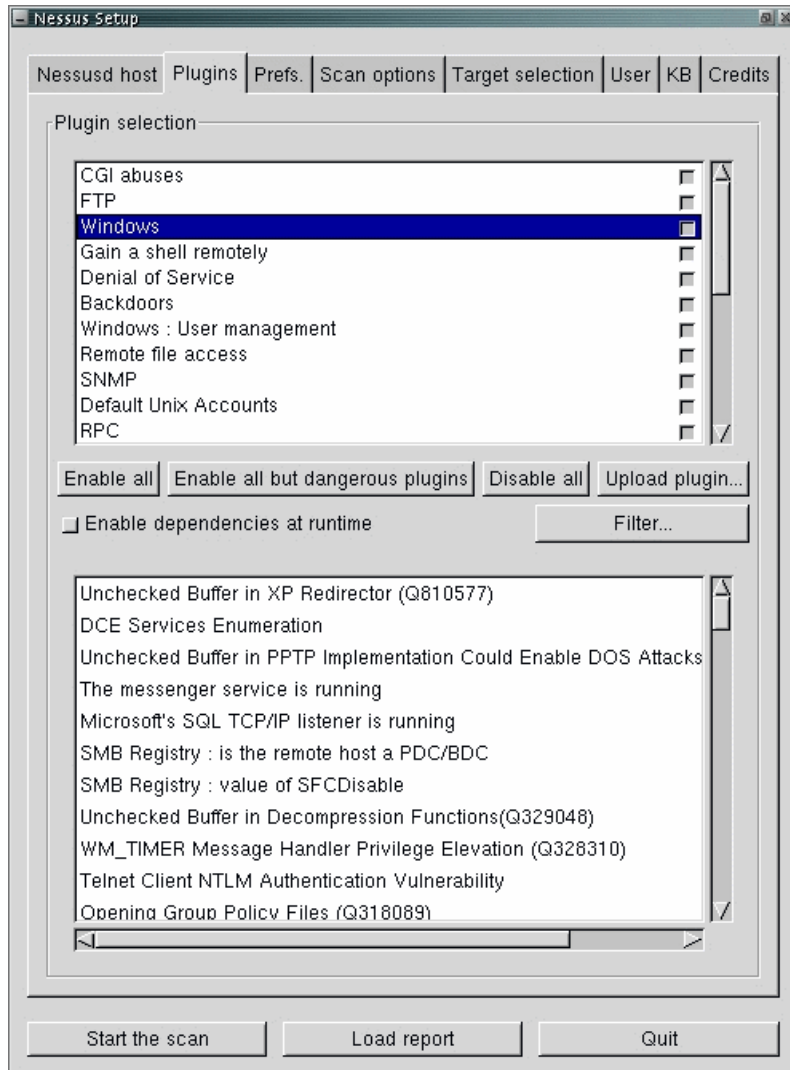
- Analyse active des vulnérabilités présentes
 - Plus ou moins agressif
 - Automatisation d'un test d'intrusion
 - Suivi
- Principaux produits existant
 - Nessus (*free software*)
 - ISS Internet Scanner
 - ...

Nessus (1)

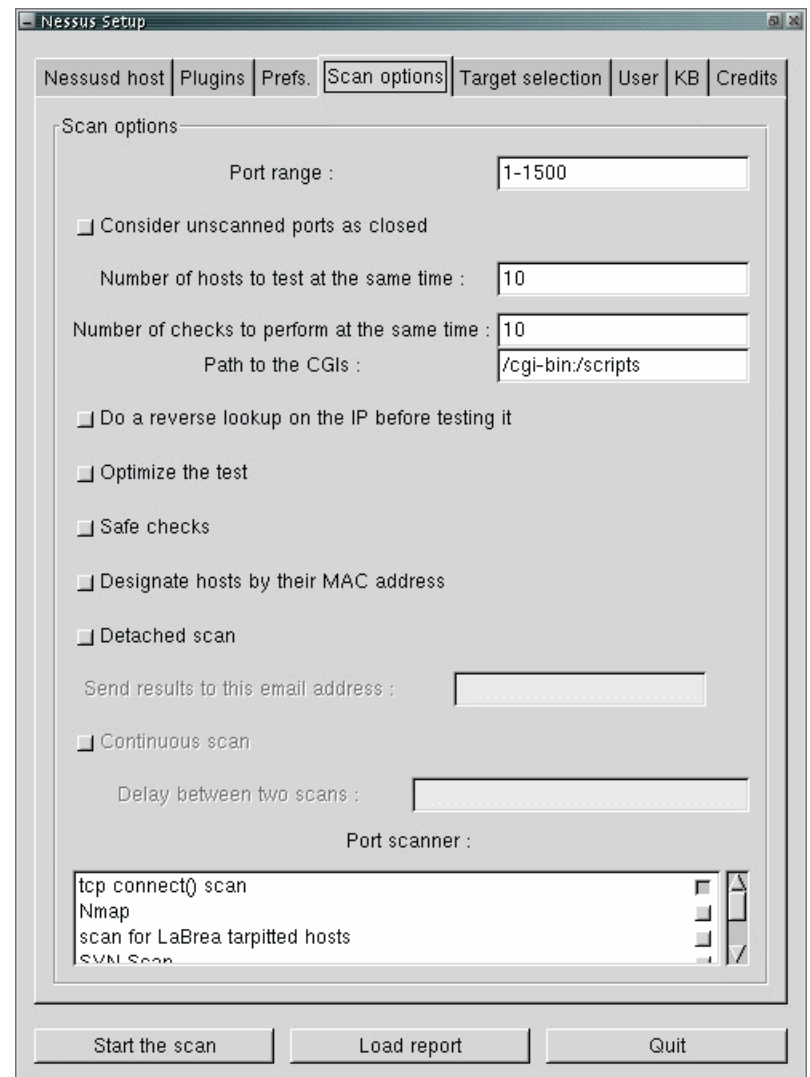
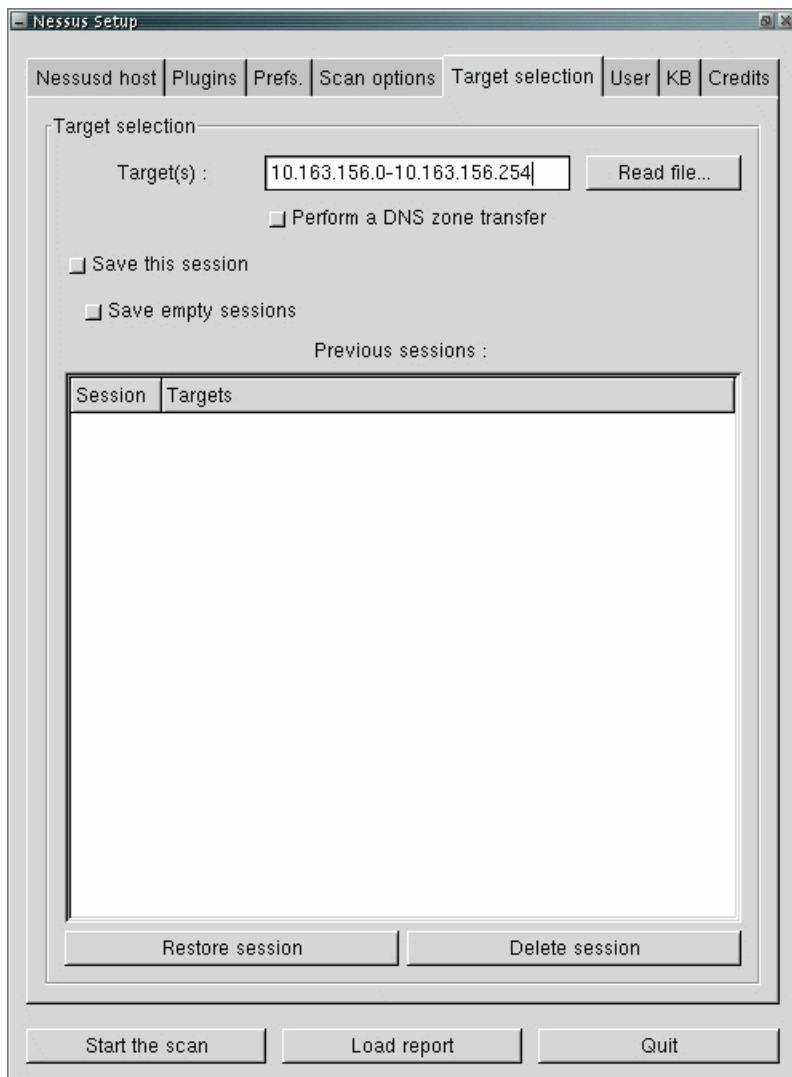
- Compilation et/ou installation (serveur, client)
- Création d'un utilisateur pour le serveur
 - # `nessus-adduser`
 - Authentification par certificat ou mot de passe
- Configuration
 - `vi /usr/local/etc/nessus/nessusd.conf`
- Démarrage du démon
 - # `nessusd -D`
 - ou `/etc/init.d/nessusd start`
- Lancer le client



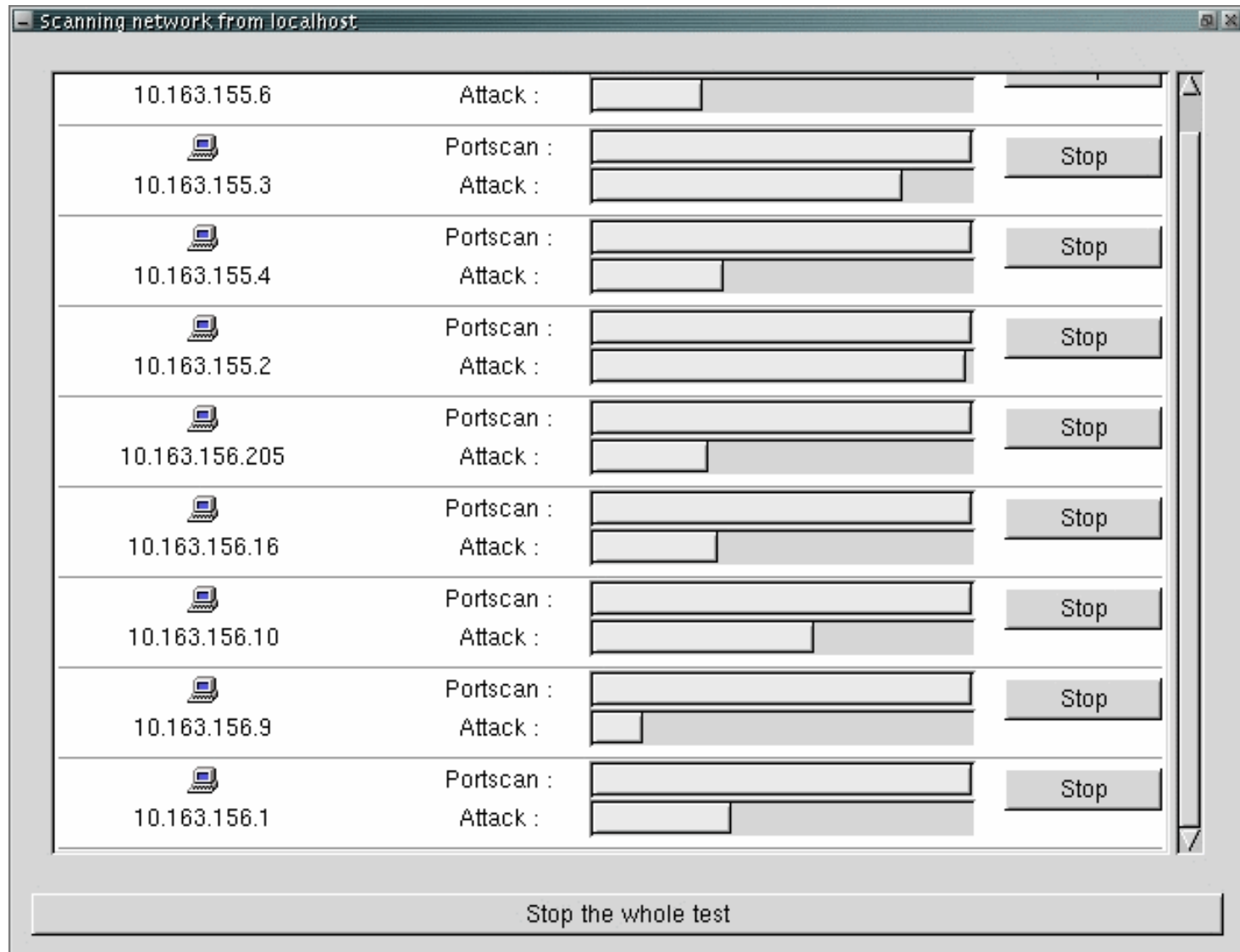
Nessus (2)



Nessus (3)



Nessus (4)



Nessus (5)

The screenshot shows the Nessus 'NG' Report interface. The 'Subnet' pane lists 10.163.155 and 10.163.156. The 'Host' pane lists 10.163.156.1, 10.163.156.9, 10.163.156.10, 10.163.156.16, and 10.163.156.205. The 'Port' pane lists various services, with 'netbios-ssn (139/tcp)' selected. The 'Severity' pane shows 'Security Warning', 'Security Note', and 'Security Hole'. The main content area displays a detailed warning for netbios-ssn on port 139/tcp, explaining that the host SID can be used to enumerate local users. It lists several users including Administrator (id 500), Guest (id 501), and various system users. The risk factor is Medium, and the solution is to filter incoming connections on this port. The CVE is CVE-2000-1200 and the BID is 959. A second warning at the bottom states that the host SID can be obtained remotely and lists the GABBO value: 5-21-842925246-1563985344-2146861395. The solution for this warning is to filter ports 137 to 139 and 445.

Subnet

- 10.163.155
- 10.163.156

Host

- 10.163.156.1
- 10.163.156.9
- 10.163.156.10
- 10.163.156.16
- 10.163.156.205

Port

- unknown (1035/tcp)
- unknown (1028/tcp)
- snmp (161/udp)
- smtp (25/tcp)
- qotd (17/udp)
- qotd (17/tcp)
- printer (515/tcp)
- nntp (563/tcp)
- nntp (119/tcp)
- netinfo (1033/tcp)
- netbios-ssn (139/tcp)
- netbios-ns (137/udp)
- nameserver (42/tcp)
- ms-term-serv (3389/tcp)

Severity

- Security Warning
- Security Note
- Security Hole

The host SID could be used to enumerate the names of the local users of this host
(we only enumerated users name whose ID is between 1000 and 1020 for performance reasons)
This gives extra knowledge to an attacker, which is not a good thing :

- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_GABBO (id 1003)
- IWAM_GABBO (id 1004)
- DHCP Users (id 1005)
- DHCP Administrators (id 1006)
- WINS Users (id 1007)

Risk factor : Medium
Solution : filter incoming connections this port

CVE : CVE-2000-1200
BID : 959

The host SID can be obtained remotely. Its value is :

GABBO : 5-21-842925246-1563985344-2146861395

An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139 and 445

Save report... Close window

Nessus (6)

- Plusieurs formats de sortie
 - Interne (.NBE, .NSR)
 - HTML (2)
 - ASCII
 - LaTeX
- Consulter www.nessus.org (la page « Démonstration »)

[Renaud Deraison *et al.*, 1998-2004]

ISS Internet/Wireless/System/Database Scanner

The screenshot displays the ISS Internet Scanner interface. The left pane shows a tree view of vulnerabilities, including items like 'adminblankpw Administrator [1]', 'NTSpooferLpcPort [1]', and several 'DCOM Config Writable' entries. The right pane shows a table of scan results for various hosts.

Host	Status	Time
StacheldrahtDos		Sat Jan 19 10:10:06
BackdoorBugs		Sat Jan 19 10:10:17
BackdoorCov		Sat Jan 19 10:10:19
BackdoorFore		Sat Jan 19 10:10:20
BackdoorWctral		Sat Jan 19 10:10:22
BackdoorRat		Sat Jan 19 10:10:23
BackdoorSocketsDeTroie		Sat Jan 19 10:11:08
HttpIndexserveAspSource		Sat Jan 19 10:11:13
OfficescanAdminAccess		Sat Jan 19 10:11:16
IsBadescapes		Sat Jan 19 10:11:19
BackdoorHostControl		Sat Jan 19 10:11:19
NetscapeServerDirector...		Sat Jan 19 10:11:21
BackdoorSwift		Sat Jan 19 10:11:24
BackdoorSnidb2		Sat Jan 19 10:11:25
BackdoorRemoteStorm		Sat Jan 19 10:11:27
BackdoorNetdemon		Sat Jan 19 10:11:28
IsChunkedEncodingDos		Sat Jan 19 10:11:30
WltpdPathDisclosure		Sat Jan 19 10:11:33
GnutellaPresent		Sat Jan 19 10:11:34
FwLocalhostAuth		Sat Jan 19 10:11:36
FwGettopoNoauth		Sat Jan 19 10:11:37
NetBusPro		Sat Jan 19 10:11:39
BackdoorChupacabra		Sat Jan 19 10:11:40
DnsBadreqCheck		Sat Jan 19 10:11:42
IqreqCheck		Sat Jan 19 10:11:54
ZoneVerCheck		Sat Jan 19 10:12:06
Traceroute		Sat Jan 19 10:12:07

The bottom pane shows a log of system messages, including: 'Database directory cannot be secured', 'Fish spoof response server bound', 'Rlogin spoof response server bound', 'Response server thread started', 'The RPC Packet Server process is being started at "C:\Program Files\ISS\Scanner\Tools\ppcdrv.exe".', 'The RPC Packet Server process has been successfully started.', 'Contacting the RPC Packet Server to make sure startup was OK.', 'The RPC Packet Server was successfully started and initialized itself properly.', 'The RPC Packet Server could not be started because the ARP gateway could not be determined. Disabling all raw packet operations.'

Mots de passe utilisés

- Étendre l'audit vers l'observation du niveau de vulnérabilité des mots de passe
- Attention à la protection des résultats
 - Il est probablement préférable de ne pas diffuser les résultats
- Associer ces résultats aux règles de gestion
 - Politique de préconisation
 - Sensibilisation
 - Règles automatiques

