Rodolfo Baader
rbaader@arcert.gov.ar

October 2005

SiMoS

Security Monitoring System

Onti Oficina Nacional de Tecnologías de Información
ArCERT Coordinación de Emergencias en Redes Teleinformáticas
Av. Roque Sáenz Peña 511 C.P. (C1035AAA) Ciudad de Buenos Aires - República Argentina

Remote vulnerability scanner Based on

Nessus + Nmap + Nikto

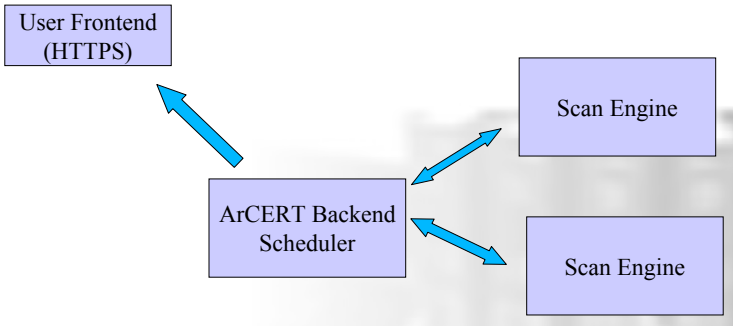
+

Web user interface

+

Scheduler

Architecture



Oficina Nacional de Tecnologías de Información
ArCERT Coordinación de Emergencias en Redes Teleinformáticas
Av. Roque Sáenz Peña 511 C.P. (C1035AAA) Ciudad de Buenos Aires - República Argentina

User frontend

backend

Scheduler
Scan Engine
Manual revision of requests and reports,
Possibility of pointing false positives

Onti Oficina Nacional de Tecnologías de Información
ArCERT Coordinación de Emergencias en Redes Teleinformáticas
Av. Roque Sáenz Peña 511 C.P. (C1035AAA) Ciudad de Buenos Aires - República Argentina

Nessus results Output File
XML, HTML, NBE, Etc.

Decided to use XML:

- More complete format
- Extensible

Problem: wasn't working properly
Solution: Fix code, commit patch (dec 2002)

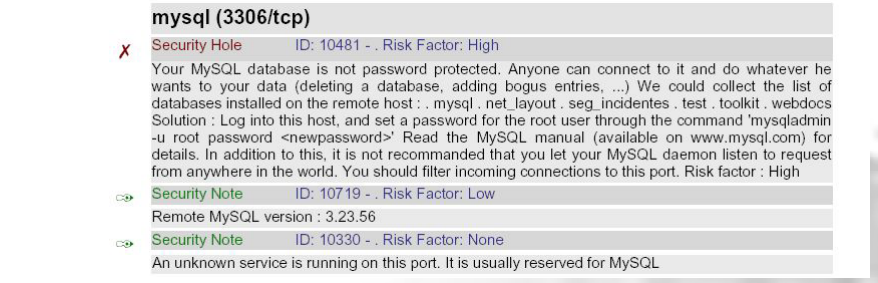
Report - briefing

DATOS del ANALISIS	
Organismo	ArCERT
Equipo Analizado	ejemplo-simos.arcert.gov.ar
Fecha Inicio	09/09/2003 10:50
Fecha Fin	09/09/2003 10:59
Puertos TCP Abiertos	8
Puertos UDP Abiertos	4
Ataques DoS Habilitado	No

PUERTOS de RED ACTIVOS				
Nombre	Puerto/Protocolo	✗ Holes	! Warnings	☞ Notes
unknown	5432/tcp	1	0	1
ssh	22/tcp	2	2	3
printer	515/tcp	0	0	1
ntp	123/udp	0	0	1
netbios-ssn	139/tcp	0	0	0
netbios-ns	137/udp	0	1	0
mysql	3306/tcp	1	0	2
http	80/tcp	1	3	5
general/tcp	/tcp	0	1	1
general/icmp	/icmp	0	1	0
domain	53/udp	0	0	1
domain	53/tcp	0	1	2
cvspserver	2401/tcp	0	1	0
bootps	67/udp	1	0	1
	Totales	6	10	18

Onti Oficina Nacional de Tecnologías de Información
ArCERT Coordinación de Emergencias en Redes Teleinformáticas
Av. Roque Sáenz Peña 511 C.P. (C1035AAA) Ciudad de Buenos Aires - República Argentina

Report - port details



mysql (3306/tcp)

✗ Security Hole ID: 10481 - . Risk Factor: High

Your MySQL database is not password protected. Anyone can connect to it and do whatever he wants to your data (deleting a database, adding bogus entries, ...) We could collect the list of databases installed on the remote host : . mysql . net_layout . seg_incidentes . test . toolkit . webdocs Solution : Log into this host, and set a password for the root user through the command 'mysqladmin -u root password <newpassword>' Read the MySQL manual (available on www.mysql.com) for details. In addition to this, it is not recommanded that you let your MySQL daemon listen to request from anywhere in the world. You should filter incoming connections to this port. Risk factor : High

Security Note ID: 10719 - . Risk Factor: Low

Remote MySQL version : 3.23.56

Security Note ID: 10330 - . Risk Factor: None

An unknown service is running on this port. It is usually reserved for MySQL

Formal Agreement

- Formal permission for doing the scan
- Requestor defines IP range
- Defines who has access to the reports
-Defines responsibilities. Disclaimer

Onti Oficina Nacional de Tecnologías de Información
ArCERT Coordinación de Emergencias en Redes Teleinformáticas
Av. Roque Sáenz Peña 511 C.P. (C1035AAA) Ciudad de Buenos Aires - República Argentina

DNSar

DNSar

Tests similar to:
www.dnsreport.com
www.zonecheck.fr

But:

Maintains historical databases of RR's and problems from our constituency
Allows statistic gathering

Onti Oficina Nacional de Tecnologías de Información
ArCERT Coordinación de Emergencias en Redes Teleinformáticas
Av. Roque Sáenz Peña 511 C.P. (C1035AAA) Ciudad de Buenos Aires - República Argentina

DNSar

1800+ gov.ar Domains

56% nameservers accept recursive queries
28% domains zone transfers allowed
45% only 1 mx record
3% forbidden cnames in MX and NS (RFC 2181)
1% include private ip addresses (RFC 1918)
16% lame delegation