6. Identificarea vulnerabilităţilor

Vulnerabilităţi

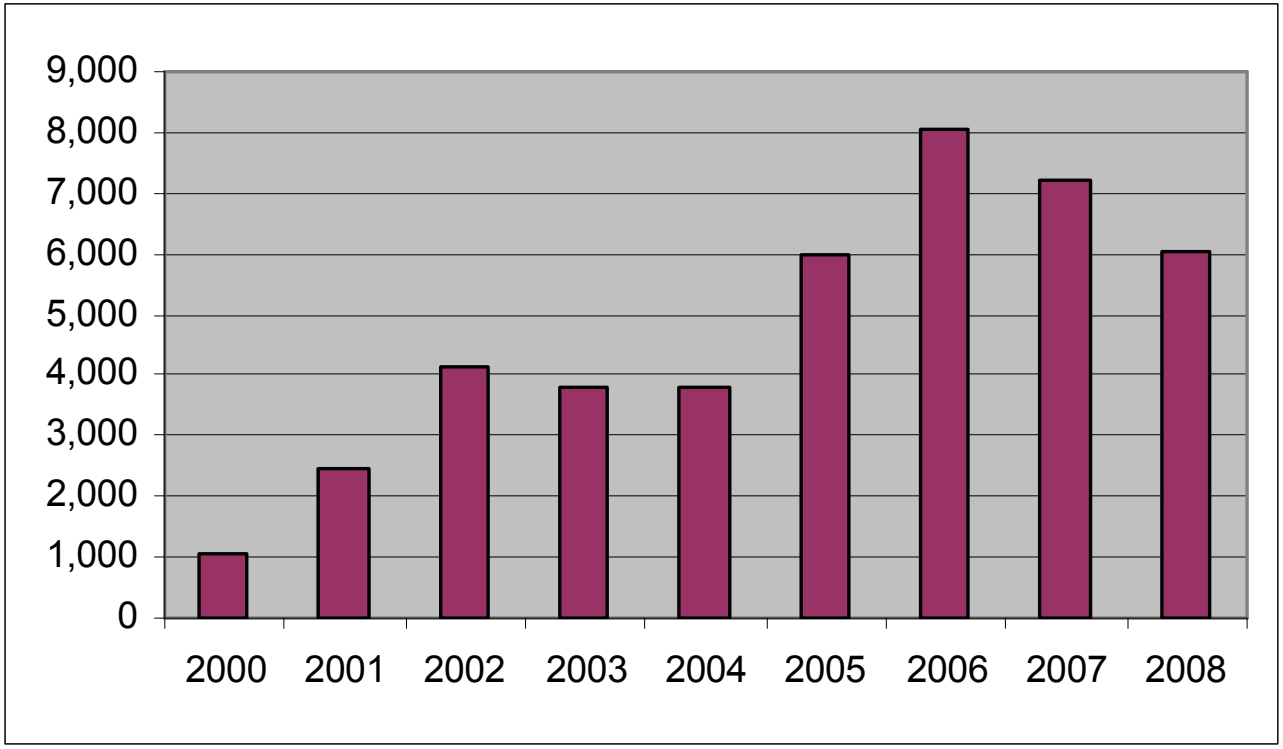
- Eroare de programare sau greşeală de configurare ce poate crea breşe în securitatea sistemelor
- Dacă nu sunt corectate la timp pot fi exploatate de către un eventual atacator
- Metode de corecţie
  - instalare de patch-uri recomandate de producător
  - securizarea sistemelor (hardening)

Vulnerabilităţi (cont.)

Total vulnerabilităţi raportate (1995-Q3,2008): 44,074

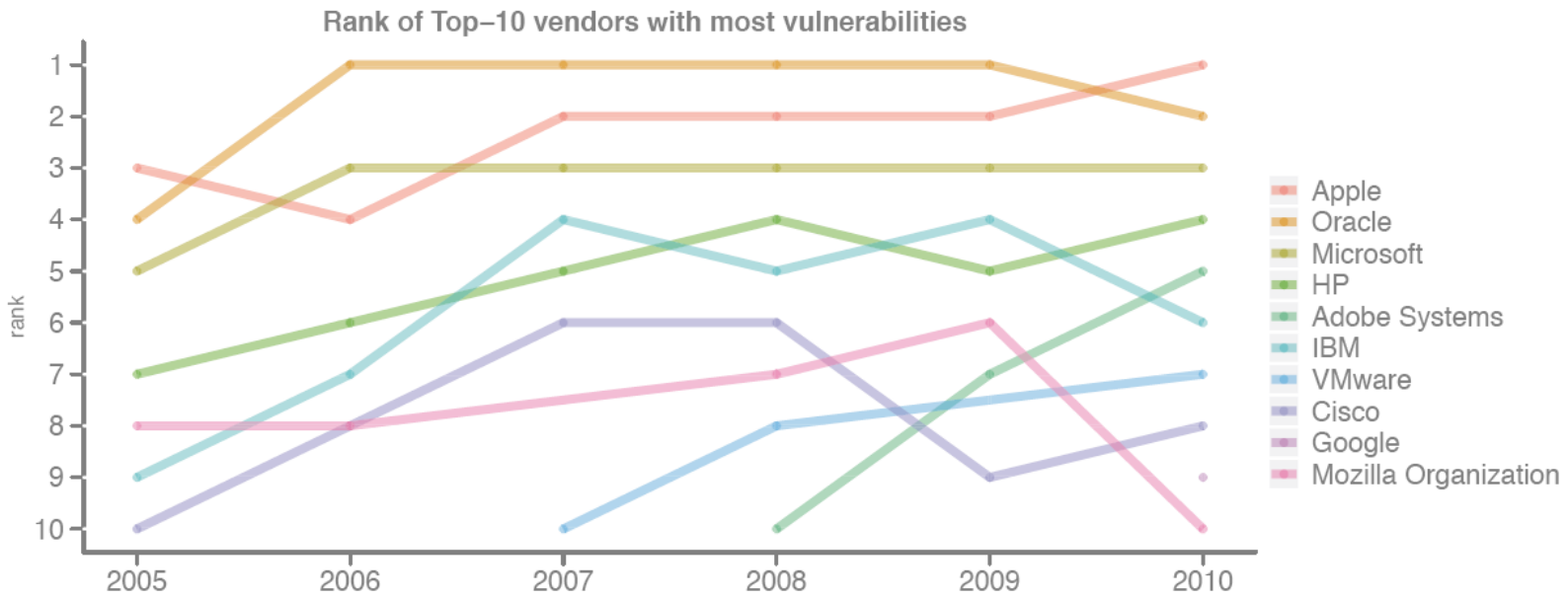
Sursa: CERT (http://www.cert.org)

Year	2000	2001	2002	2003	2004	2005	2006	2007
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064	7,236



Vulnerabilităţi (cont.)

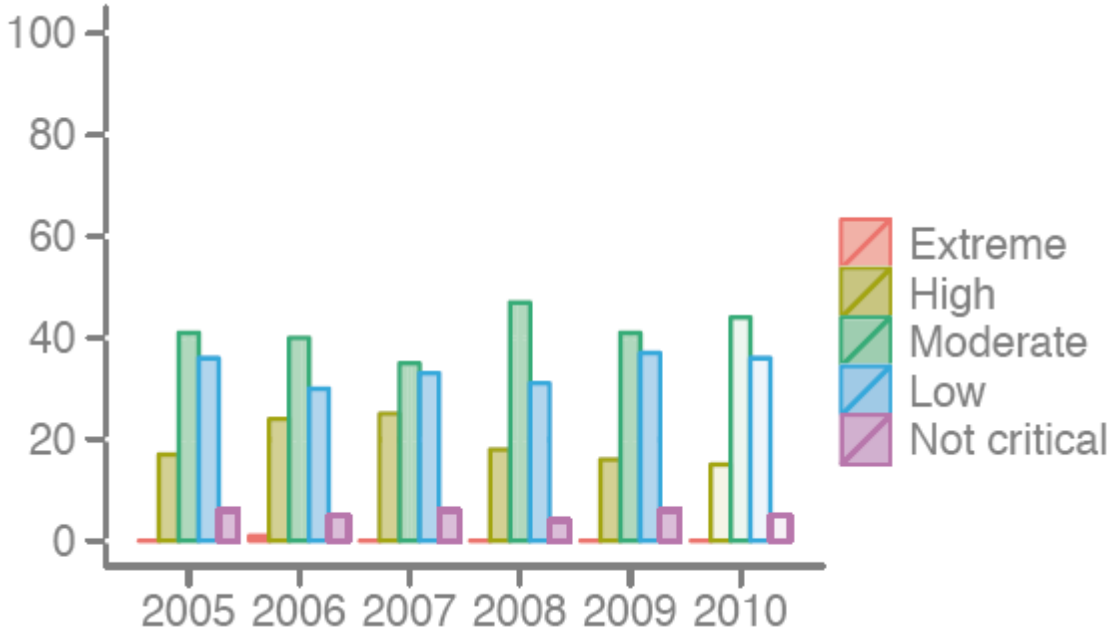
10 firme sunt responsabile pentru 38% din vulnerabilităţile dintr-un an!



Sursa: Secunia (http://www.secunia.com)

Vulnerabilităţi (cont.)

Numai 20% din vulnerabilităţi sunt critice!



Sursa: Secunia (http://www.secunia.com)

Vulnerabilităţi (cont.)

- Common Vulnerabilities and Exposures (CVE)
  - lista cu denumirile standardizate ale tuturor vulnerabilităţilor cunoscute public
  - dicţionar de vulnerabilităţi (nu bază de date)
  - http://cve.mitre.org/
- Open Vulnerability and Assessment Language (OVAL)
  - standard ce descrie modul în care poate fi verificată existenţa unei vulnerabilităţi pe un sistem de calcul
  - http://oval.mitre.org/

Scannere de vulnerabilităţi

- Automatizarea procesului de identificare şi corectare a vulnerabilităţilor
- Clasificare
  - funcţie de locaţie de unde se face scanarea
    - network based
    - host based
  - funcţie de credenţialele folosite pe parcursul scanării
    - cu drepturi administrative
    - fără drepturi administrative
  - funcţie de tipul de sisteme / aplicaţii testate
    - de uz general
    - pentru aplicaţii web

Scannere de vulnerabilităţi de uz general

- Nessus (http://www.nessus.org)
  - the best security tool!
- SARA - Security Auditor's Research Assistant (http://www-arc.com/sara/)
- X-scan (http://www.xfocus.com)
- MBSA (http://www.microsoft.com)

- GFI LANGuard (http://www.gfi.com)
- Retina (http://www.eeye.com)
- CORE IMPACT (http://www.coresecurity.com)
- Proventia Network Enterprise Scanner (http://www.ibm.com)
- QualysGuard (http://www.qualys.com/)
- SAINT - System Administrator's Integrated Network Tool (http://www.saintcorporation.com/)
- …

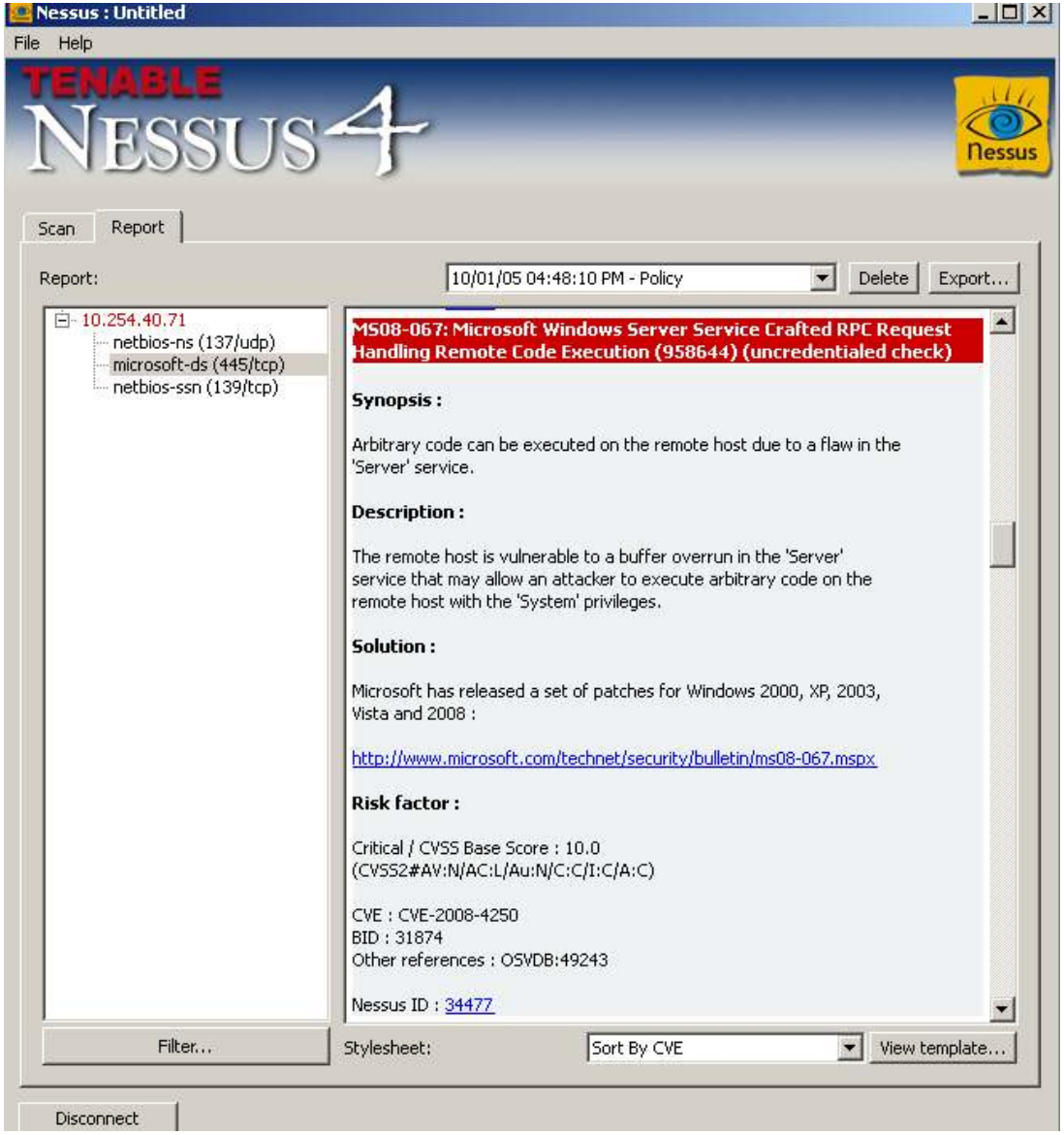
Nessus

- Arhitectură client / server
  - server (scanning engine)
  - client (user interface)
  - autentificare utilizatori + criptare conexiune (SSL)
- Modular
  - funcţionalităţi implementate sub forma de plugin-uri (script-uri)
  - aproximativ 40.000 de plugin-uri de scanare a vulnerabilităţilor
  - NASL (Nessus Attack Scripting Language)
- Detectarea serviciilor active de pe calculatorul ţintă se face prin port scanning
  - ping, TCP connect(), SYN scan
- Metode de scanare safe / distructive
- Generare de rapoarte (HTML)
- Compatibil CVE
- 2 tipuri de abonamente
  - ProfessionalFeed (1200 USD / year)
  - HomeFeed (free)

Nessus (cont.)

1. Conectare în sistem (autentificare)
2. Definire ţinte (calculator / subreţea)
3. Selectare politică de scanare (plugin-uri)
4. Scanare sisteme
5. Interpretare rezultate

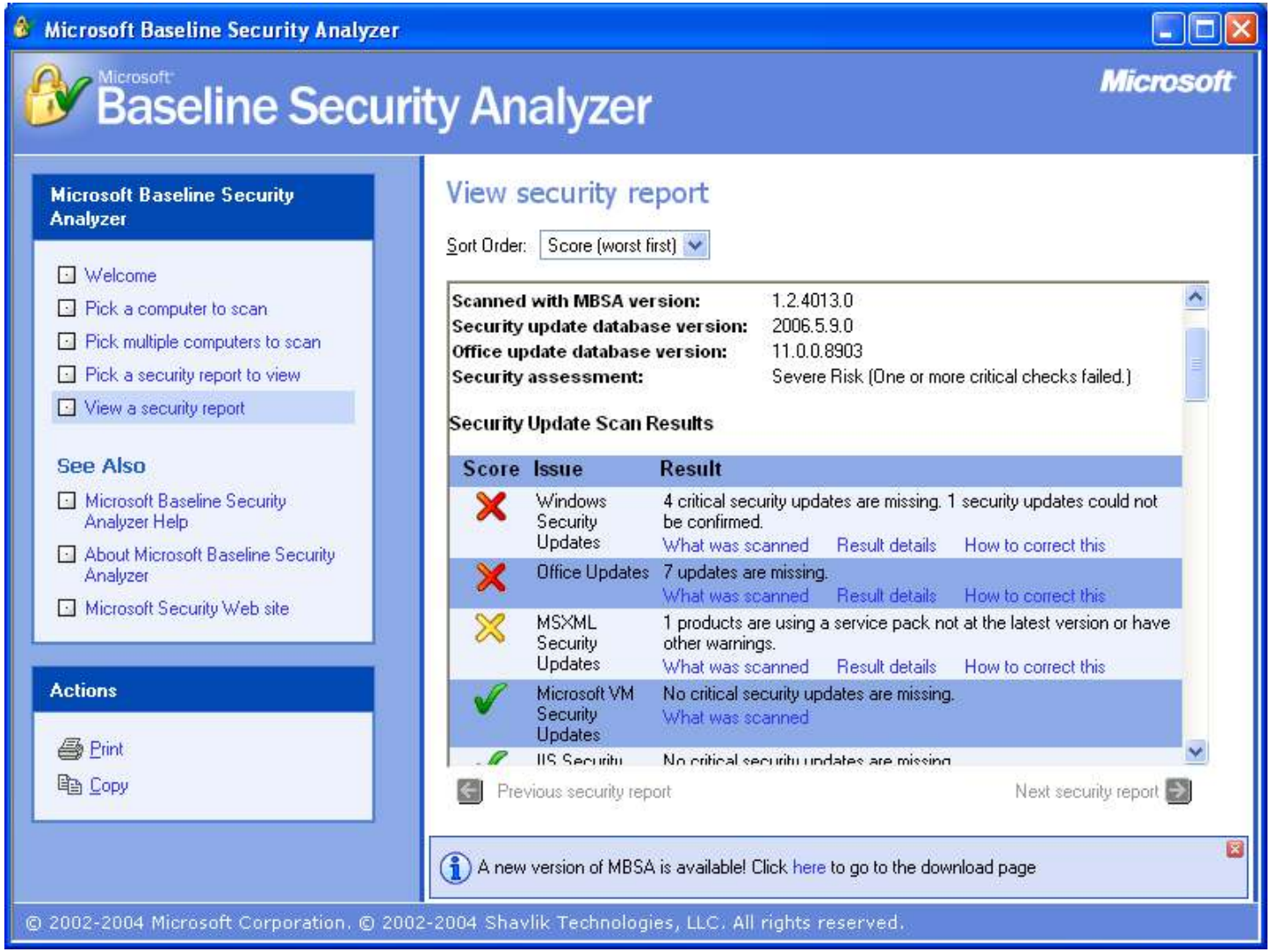
Nessus (cont.)



MBSA

- Microsoft Baseline Security Analyzer
- Detectează vulnerabilităţi specifice produselor Microsoft:
  - Security updates
  - Weak passwords
  - Windows configuration
  - IIS vulnerabilities
  - SQL vulnerabilities
- Necesită drepturi administrative pe calculatorul ţintă
- Generare de rapoarte

MBSA (cont.)


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
View security report
Sort Order: Score (worst first)
Scanned with MBSA version: 1.2.4013.0
Security update database version: 2006.5.9.0
Office update database version: 11.0.0.8903
Security assessment: Severe Risk (One or more critical checks failed.)
Security Update Scan Results
Score Issue Result
Windows Security Updates
4 critical security updates are missing. 1 security updates could not be confirmed.
What was scanned Result details How to correct this
Office Updates
7 updates are missing.
What was scanned Result details How to correct this
MSXML Security Updates
1 products are using a service pack not at the latest version or have other warnings.
What was scanned Result details How to correct this
Microsoft VM Security Updates
No critical security updates are missing.
What was scanned
Previous security report
Next security report
A new version of MBSA is available! Click here to go to the download page
© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Vulnerabilităţi specifice aplicaţiilor Web

"Over 70% of security vulnerabilities exist at the application layer, not the network or system layer."

– Gartner 2004-2006

Vulnerabilităţi specifice aplicaţiilor Web (cont.)

- Unvalidated Input
- Cookie Poisoning
- CGI Parameters
- SQL Injection
- Cross site scripting (XSS)
- Directory Traversal
- Buffer Overflow
- …

Scannere de vulnerabilităţi pentru aplicaţii Web

- Nikto (http://www.cirt.net/nikto2)
- Paros proxy (http://www.parosproxy.org)
- Burpsuite (http://portswigger.net/suite/)

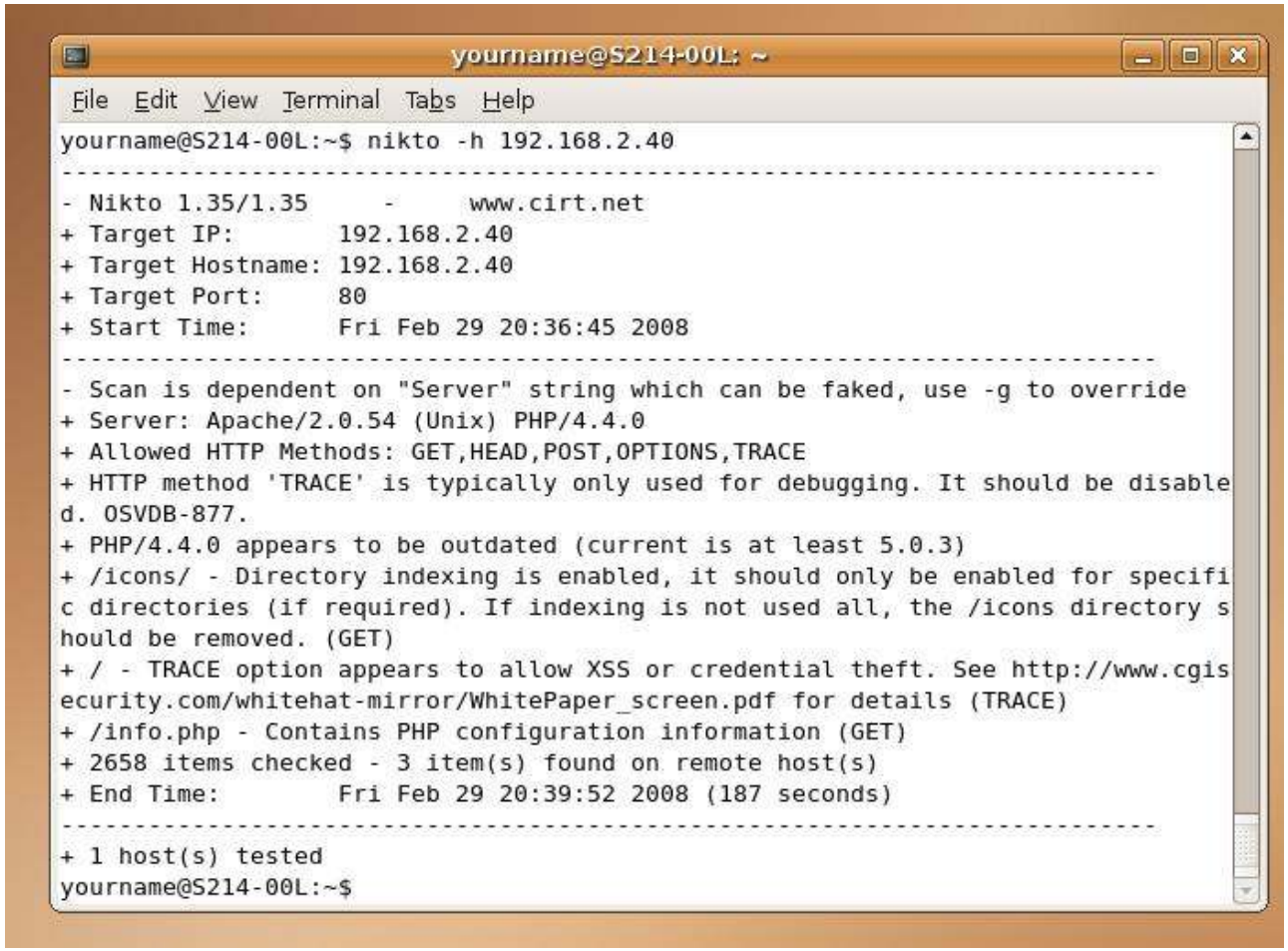
- WebInspect (http://www.spidynamics.com)
- Acunetix WVS (http://www.acunetix.com)
- Rational AppScan (http://www.ibm.com)
- N-Stealth (http://www.nstalker.com/nstealth/)

- Open Web Application Security Project (OWASP)
  - http://www.owasp.org/

Nikto

- Open Source (GPL)
- Utilitar în linie de comandă
- Verificări efectuate:
  - server and software misconfigurations
  - default files and programs
  - insecure files and programs
  - outdated servers and programs
- Asigură identificarea modulelor software instalate pe serverul de Web (php, perl, etc)
- Suport pentru SSL, LibWhisker2 (anti IDS)
- Generare rapoarte în diverse formate (text, CSV, HTML, XML, NBE)
- Permite integrarea cu Nessus
  - lansarea automată a programului nikto atunci când Nessus detectează un server de Web

Nikto (cont.)



Acunetics WVS

- Verificări efectuate:
  - CGI testing
  - parameter manipulation (SQL Injection, XSS, …)
  - text search
  - port scanning
  - Google Hacking Database
- Generare de rapoarte customizate
- Suport pentru AJAX / Web 2.0
- Suport pentru CAPTCHA, Single Sign-On şi mecanisme de autentificare bazate pe doi factori
- Unelte auxiliare
  - HTTP Editor, HTTP Sniffer, HTTP Fuzzer, Scripting tool, Blind SQL Injector
- 1500 USD (Single User Single URL Perpetual License)

Acunetics WVS (cont.)