

NeXpose Vulnerability Scanner

December 2008 Security SIG

Melissa Muth

ISC Information Security

Capabilities

- Remote vulnerability scanning:
 - OS: Microsoft Windows, Linux, Solaris, Mac OS, BSD, AIX, AS/400
 - Databases: SQL Server, MySQL, Oracle, PostgreSQL
 - Web: Apache, IIS, QuickTime, Flash, ColdFusion, J2EE, PHP, ASP, ASP.NET

Capabilities (con't)

- Custom web app issues: SQL injection, cross-site scripting, backup script files, readable CGI scripts, insecure use of passwords, leakage of sensitive data
- Device discovery and fingerprinting
- Web spidering
- Default or trivial account credentials

Capabilities (con't)

- Credentials-based scanning
 - Vulnerabilities
 - Insecure configurations
 - Missing patches
 - Spyware
 - OS: Red Hat, SuSE, Solaris, Microsoft
 - Applications: Microsoft products, Real Player, Opera, OpenOffice, etc.

Benefits

- Low false-positive rate (handled as bugs)
- Three checks done for each vulnerability
- Flexible reporting (PDF, HTML, XML, etc)
- No local software required (browser-based)
- Separate scanning engine for firewalled hosts

NeXpose at Penn

- Scanning appliance: <https://scanner.security.isc.upenn.edu:3780/>
- Floating scanning engine license
- PennKey authentication
- Network Discovery licenses: 4 class B networks
- Host scan licenses: 1250 total
 - Critical hosts: 800
 - OACP: 250
 - Floating: 200

ISC Roles

- Regular scans of Critical Hosts
- Define Sites (sets of devices) and Site Administrators (LSPs) to share 200 floating host licenses
- Subject to change:
 - NeXpose 5.0 to provide more granular access
 - NeXpose API could be used to develop front-end
- Coordinate pairing of floating scanning engine with NeXpose Console

Site Administrator Roles

- Provide ISC with list of hosts to be scanned
- Provide ISC with list of authorized users
- Select type of scan to be run
- Set up alerts
- Configure credentials (optional)
- Initiate and schedule scans
- Generate reports

Floating Scanning Engine

- Ideal for scans behind firewalls
- Requirements
 - Windows 2000 Server, Windows 2003, Linux
 - 2 GHz, 2 GB RAM, 80 GB disk
- Initial pairing with NeXpose console: contact ISC
- Subsequent use: advisory scheduling via ProWiki
 - <http://prowiki.isc.upenn.edu/wiki/Category:Scanning>

ISC To-Do Items

- Web site for NeXpose service
 - Overview, ISC/LSP roles & procedures
 - Scanning engine software, install/config info
 - Details of scan templates
 - XML to CSV converter
 - Sign-up for user group mailing list
- Work with you to create new templates as needed
- Request to vendor: brute force countermeasure check

Next Steps (LSPs)

- Send to security@isc.upenn.edu:
 - Site definitions (hosts to be scanned & how)
 - Authorized users for each
 - Asset groups (for reporting)
- Use ProWiki to advise others of scheduled or planned scans
- Contact us to set up floating scanning engine

NeXpose

- Thank you for attending!
- Questions?
- Requests?