Vulnerability Scanning: a research report and best practices

By
Daniel Ferrer
(Central Michigan University Libraries)

Doug Randall
(VP Product Technology
Innovative Interfaces, Inc.)

May 2007
IUG 15 San Jose

What is the basic idea?

Find vulnerabilities by you attacking your libraries' III server.

To use software, so you can attack your own libraries' server and find vulnerabilities before hackers find them, so you can fix them first.

Schedule them once a month or after major upgrades. Depending upon your risk level (size, credit cards information) and resources.
A little paranoia will help keep your computer systems safe.

The main aim of scanning is to identify technical weaknesses/vulnerabilities in III server; and then prioritize them based on the importance and work toward determining how the vulnerabilities should be fixed.

Easy to setup and use

The scanning software is easy to setup and use and in fact it is getting easier to download and start using.

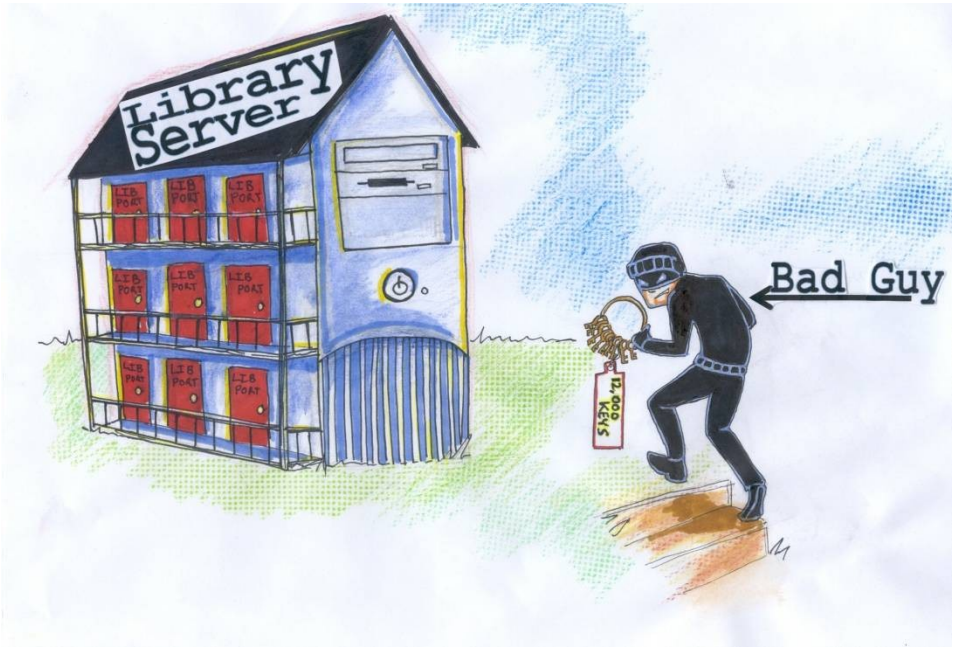
‘Script kiddies’ to scan and look at a large number of computer systems by IP number range while the rest of us are sleeping.

No programming required.

No degree in Computer Science is needed.

Used by serious criminals to begin more serious attacks.

Vulnerability Scanning



Patron privacy

Patron privacy – is crucial and very important, TRUST!!

Legal issues: IFLA (Glasgow Declaration on Libraries, Information Services and Intellectual Freedom, 2002), ALA ethics, state laws, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Family Educational Rights and Privacy Act (FERPA).

Privacy: even USA and British law are different "divulging confidences". Other nations? USA's legal definition general based recently on tort scholar, William L. Prosser. Recent example, Medical information protected by HIPPA Laws. HIPPA laws that include individual fines and jail time for individuals. Libraries need toward this level of security.

In providing services to patrons, patrons must be able to trust librarians to maintain confidentiality. Indeed, patron privacy is protected by laws as well as our ethics. Over the doors of libraries should be written "Privacy Protected". Fine print details.

Ownership of your III server

Beside patron privacy, the other central issue with computer security is the ownership of your III server. You "own" your III server and hence you do not one someone else taking it over and using for their own purpose. For example, spam e-mail and video sharing software.

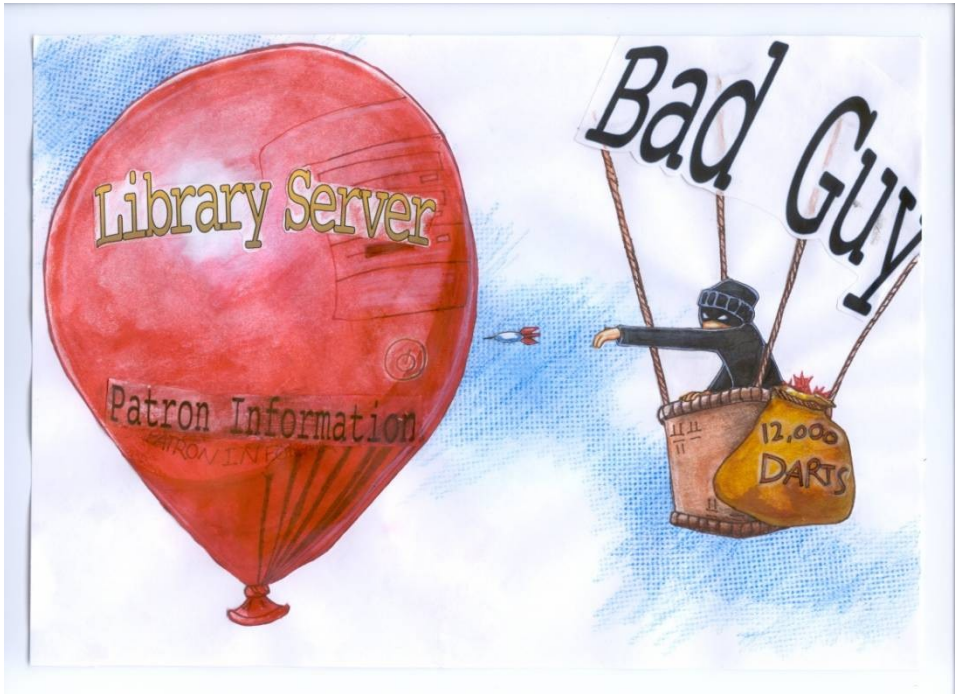
Data Breaches, including some libraries. 30 states have passed laws requiring that individuals be notified of security breaches. 150,000,000 sensitive personal information records lost detailed here: http://www.privacyrights.org/ar/ChronDataBreaches.htm

First steps

III Solution: go to “LOGIN names & parameters”, then “Limit NETWORK Access” and review all of the setting and think about restricting access to these applications by IP number range. Build the walls higher.

Software only sites. Patch management. Shutdown extra inetd.conf services. Use TCP wrappers. Security is extra important !

Vulnerability Scanning



Open Ports - services

OPEN PORTS like open doors in your house.
You need some open ports for network traffic/services.

Network Services go through Open Ports, some general example:

HyperText Transfer Protocol [http] (80), HTPS - HTTP Protocol over TLS/SSL (encrypted transmission) (port 443), telnet (23), ftp (21), SSH (22).

Read the III documentation about the ports!

Examples of the III ports

- Millennium Client (2000), Self Checkout (5550), Web Access Management Server -WAM (8080), Circulation Statistics Web Report (4441).

- Use the documentation from III about the assignment of the ports on their system: http://csdirect.iii.com/faq/firewall.shtml

Major Caveat

These scanners can actually crash a computer/server and you need to get the “legal” owner’s permission before scanning any computer (sticky issue if there is a problem). Do not scan other people’s/libraries servers (even if they give permission), since this may be considered illegal by the network owners and server’s legal owners. If there is a problem!!

Be careful with vulnerability reports (kept them locked up), since they show hackers how and where to attack you. Do not send them unencrypted over e-mail as attachments.

Version rollback attacks

Example: 1). Version rollback attacks.

Most upgrades include security fixes, so if you are supporting the much earlier version of the software, then you most likely are open to attacks of the earlier versions.

SSH (port 22/tcp)

The remote SSH daemon supports the following versions of the

SSH protocol : . 1.33 . 1.5 . 1.99 . 2.0

Version rollback attacks

III Solution work with HELP DESK to disable earlier version of SSH and upgrade client software, so they only connect with . 2.0 See also: http://csdirect.iii.com/faq/ssh_faq.shtml

Use SSH-2 (secure shell). Connect to the III server with a SSH client, for example, PuTTY is a free Telnet/SSH Client or AnzioWin, or Anzio Lite version now comes with SSH support. Solution work with HELP DESK to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

See also: http://csdirect.iii.com/faq/ssl.shtml

Setting passwords

Example: 2. Setting passwords. A university library system example, not an III system!

ncube-lm (1521/tcp)

The remote Oracle tnslsnr has no password assigned.
An attacker may use this fact to shut it down arbitrarily,
thus preventing legitimate users from using it properly.

III Solution. Remember either not setting passwords (above example) or using weak passwords that are never changed is a security problem.
See also: http://en.wikipedia.org/wiki/Password_cracking
Turn off the “The auto-login wizard” in Anzio.

Restrict access

Example: 3. Restrict access by IP number ranges. Features and functions. Services.

telnet (23/tcp) Synopsis

Disable this service and use SSH instead.

Port scanning software will also note port 23 is open and tell you to switch to SSH (port 22), which uses encryption between your workstation and the III server.

III Solution go to “LOGIN names & parameters”, then “Limit NETWORK Access” and review all of the setting and think about restricting access to these applications by IP number range. Fine tune your security settings by IP numbers!

Limit access

Example: 4. Limit access by IP number range.

ftp (21/tcp)

The remote host is running wu-ftpd 2.6.2 or older. There is a bug in this version which may allow an attacker to bypass the 'restricted-gid' feature and gain unauthorized access to otherwise restricted directories.

III Solution go to “LOGIN names & parameters”, then “Limit NETWORK Access” and review all of the setting and think about restricting access to FTP (other applications) by IP number range.

Use SSL

Example: 5. Use SSL and keep it up to date.

https (443/tcp)

The SSL certificate of the remote service expired Jan 28 23:59:59 2006 GMT!
Plugin ID : 15901

Port is open Plugin ID : 11219
A SSLv2 server answered on this port
Plugin ID : 10330.

Use SSL part II

Second Part=Example: 5. Use SSL and keep it up to date.

https (443/tcp)

III Solution work with HELP DESK to setup SSL for you MY ACCOUNT, etc.

Note: SSL certificates costs about $300 dollars per year.

Example: from VeriSign, Co. you can purchase a certificate.

http://www.verisign.com/

FALSE POSITIVES

Example: 6. Knowledge of the system. Mixed information. Worth checking on.

The server name is right but: The remote host is NOT running the ASP Portal CGI suite.

Hence, no problem or vulnerability. FALSE POSITIVES – knowledge of the system.

The remote web server type is :
III 100 Plugin ID : 10107

FALSE POSITIVES

part II

III Solution: read the Innovative Interface Inc documentation on their use of ports. (http://csdirect.iii.com/faq/firewall.shtml).

Then check the standard documentation about the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports Assignments.

Trust but verify!

Example 7. Some good news! is also reported as well.

This means your security is in place and is really working from outside attack. Trust but verify.

ssh (22/tcp)

Port is open
Plugin ID : 11219

The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper
Plugin ID : 10330

Best Practices 1-4

Using Scanning Vulnerabilities on yours Libraries' III server.

1). Talk with your networking group first about your intentions of using a scanner.

2). Figure out a schedule. Monthly and/or after upgrades. Best to scan the server at low usage.

3). Determine who the legal owner of the server is and get written permission for scanning (in the best possible legal world). Do not scanner other servers.

4). General recommended software is Nessus. Download and setup. Do not use the denial services setting (listed on the menu as dangerous), because of network traffic issues.

Best Practices 5

5). The general issue of your scanning computer is “within” or “external”. The best case scenario is to scan your III server within the castle walls. Your computer IP number lets you access Millennium etc; so you would be inside the walls. So, your worst case is when someone is inside your campus, library building, or city network IP number range, etc.

Best Practices 6-7

6). Run scan against the III server at low usage time. May lockup or slow down the III server, especially if you have an older server.

7). Remember the report should be locked up or on a password protected computer. The report could be used by a hacker as an outline of how and where to attack your III server. Handle with care! Afterwards shredded report. Cross-cut, smallest size: 1/32" x 1/2".

Best Practices 8-10

8). Analyses of report: work with III Help Desk to fix problems. Or, if you are software only site, then review the report with the system administrator of the III server to determine what needs fixing and when to fix it. Always make documentation.

9). Make changes and see if there is way to test the change, which might include re-running the scanner software to see if the security changes worked.

10). Trust but verify. Repeat as needed.

Innovative: On Port Scanning

- Good Idea? Yes.
- Why? Only way to be sure what's open from where.
- Huge Report, Send to Help Desk? No.
- Port Scanners (even Nessus) are notoriously verbose
- Often speciously over-describing dozens of specific vulnerabilities, when they might only know a port is open.

Innovative: Parsing the Report

- Scanners are describing *potential* vulnerabilities, based on a very simple test, like whether port is listening at all
- Many 100% Innovative application programs run on ports normally used for other popular services
- Scanners assume the port really is the better known service and mistakenly list all the vulnerabilities known for that service

Innovative: What to do?

- Read the Port Scanning FAQ on CSDirect
- Report only Actionable and Legitimate
- The key test for “legitimacy” is to manually confirm the actual vulnerability is exploitable
- Gives example of testing for cgi-bin vulnerabilities against Millennium’s purpose built Web OPAC

Innovative: What to do?

- Lot of work to test each vulnerability
- Yes, but that is the next step, the scanner is just a reporting tool to find *potential* vulnerabilities.
- Where to focus?
- You can largely dismiss reports against services which are in the Innovative Firewall FAQ as obviously Innovative application like Web Reports and Web Access Management
- Ports running standard Unix services as such are more interesting (SSH, Telnet, FTP, etc.)

Innovative: What to do?

- As much as I'd like, I don't think I will be drilling down into every reported item, is there a "higher level" interpretation of the reports?
- Yes, on a port-by-port basis, you can track what is "open" versus what you think should be open from reading the Firewall FAQ
- Yes, you can establish a baseline of what ports are usually listening and note any *new* ports listening (always cause for concern)

Innovative: Other Tips?

- Scanners are a great tool to confirm what is open through your organization’s firewall
- Compare inside scan to outside scan

Innovative: A Few Statistics

- Tested a few services for all systems from “the Internet” (not special III addresses)
- To see which were blocked at institutional firewalls
- Even “open” services by this measure are likely wrapped by Limit Network Access or other measures

Innovative: Telnet 52% Open

- 52% Open At the Firewall
- OK, many of you use Telnet for staff access, but still should be blocked at the firewall
- “But we offer public Telnet”?
- Why?

Innovative: FTP 47% Open

- 47% of systems have FTP inbound allowed from the Internet
- Even if FTP is required for some partners or special cases, why have open to Internet at large?

Innovative:TCP 1031 42% Open

- Arbitrary Inno-port
- Intended to be “Staff Only”
- Good news is, 42% open is 58% closed
- That’s still not great news
- Use the CSDirect Firewall FAQ to understand which ports go with which products
- Only open necessary ports

Web Resources I

Nessus Vulnerability Scanner (version 3.0.5)

http://www.nessus.org/

http://en.wikipedia.org/wiki/Nessus_(software)

Nmap (version 4.20)

http://insecure.org/nmap/ & http://en.wikipedia.org/wiki/Nmap

SuperScan (version 4.0).

http://www.foundstone.com/ (look under Resources, free tools) http://en.wikipedia.org/wiki/Superscan

Web Resources II

Security Auditor's Research Assistant (SARA) version 7.3.1.
http://www-arc.com/sara/

General overview of scanning from Educause:
http://www.educause.edu/NetworkandHostVulnerabilityAssessment/1259

Security Administrator Tool for Analyzing Networks (SATAN first 1993)
Now replaced by newer ones. Dan Farmer and Wietse Venema.
http://en.wikipedia.org/wiki/Security_Administrator_Tool_for_Analyzing_Networks

COMMERICAL SCANNING COMPANIES

FoundScan from Foundstone
http://www.foundstone.com/

III Documentation

Innovative Interfaces, Inc. Documentation to be READ:

Using Port Scanning Software
http://csdirect.iii.com/faq/portscan.shtml

Access through Local Firewalls
http://csdirect.iii.com/faq/firewall.shtml

SSL Certificates and SSL in WebPAC
http://csdirect.iii.com/faq/ssl.shtml

Well Known Ports

- http://www.iana.org/assignments/port-numbers_
- http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Book References

Nessus, Snort, & Ethereal power tools : customizing open source security applications /
Neil Archibald; Gilbert Ramirez; Noam Rathaus, 2005
English Book xxvi, 445 p. : ill. ; 24 cm.
Rockland, MA: Syngress ; [Sebastopol, Calif.] : Distributed by O'Reilly Media, ISBN: 1597490202, 9781597490207

Nessus network auditing /
Renaud Deraison, 2004
English Book. xxix, 508 p. : ill. ; 24 cm. + 1 CD-ROM (4 3/4 in.).
Rockland, MA : Syngress, ISBN: 1932266976, 9781932266979

Book References

Book Reference:

Secure your network for free: using Nmap, Wireshark, Snort, Nessus, and MRTG / Eric Seagren; Wesley J Noonan, 2006 English Internet Resource Computer File 1 v. Rockland, Mass. : Syngress; Oxford : Elsevier Science [distributor], ; ISBN: 9781429455435 (electronic bk.) 1429455438 (electronic bk.)

Gray hat hacking: the ethical hacker's handbook / Shon Harris ... [et al.] Pub New York: McGraw-Hill/Osborne, c2005.

Final questions?

Vulnerability Scanning:
a research report and best practices
Trust but verify!!

Questions?

E-mail: Daniel.Ferrer@cmich.edu
or
E-mail:doug@iii.com

May 2007
IUG 15 San Jose