Penetration Testing and Vulnerability Scanning

Presented by

Steve Spearman
• VP of HIPAA Compliance Services, Healthicity
• 20 years in Health Information Technology
• HIPAA Expert and Speaker

Disclaimer: Nothing in this presentation should be construed as legal advice nor relied upon as legal expertise.

What is HIPAA?
HIPAA is...

- Law that governs a person’s ability to qualify immediately for health coverage when they change employment (dependent on employer’s program)
- Rules for Data Interchange
- Regulations protecting the security and privacy of Protected Health Information (PHI)

To whom does it apply?

Covered Entities*
- Health Care Providers
- Health Care Clearinghouse
- Health Plan

Business Associates**

*Covered Entities: Dr. related to Claims, Verification, Referrals, Status, Enrollment, Payment, Remunors, coordination of benefits

**Contractor or vendor, not involved in patient care, that requires access to PHI in order to fulfill the duties of the contract

Obligations of Business Associates

1. Comply with the HIPAA Security Rule
2. Report to Covered Entity and breach of unsecured PHI
3. Enter into BAA with subcontractor imposing the same obligations that apply to the Business Associate
4. Comply with the HIPAA Privacy Rule to the extent Business Associate is carrying out a Covered Entity’s Privacy Rule obligations (e.g., accounting of disclosures, request for amendments, etc.)
The Three Essential Elements of a HIPAA Compliance Program

- Security Risk Analysis
- Policies and Procedures
- Training

CIA: Confidentiality Integrity Availability

Confidentiality: The property that data or information is not made available or disclosed to an unauthorized person.

Integrity: The property that data or information has not been altered or destroyed in an unauthorized manner.

Availability: The property that data or information is accessible and useable upon demand by an authorized person.

Structure of the Security Rule

<table>
<thead>
<tr>
<th>Standards</th>
<th>Implementation Specifications</th>
<th>(R) Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
<td>(R)</td>
</tr>
<tr>
<td>Management</td>
<td>Risk Analysis</td>
<td>(R)</td>
</tr>
<tr>
<td>Process</td>
<td>Sanction Policy</td>
<td>(R)</td>
</tr>
<tr>
<td></td>
<td>Information System Activity</td>
<td>(R)</td>
</tr>
</tbody>
</table>

Security Standards Matrix (Appendix A of the Security Rule)

- The standards are “Required”
- Implementation Specifications:
  - The more detailed instructions contained within each Standard
  - Some are required (R)
  - Some are addressable (A) – flexibility and latitude in meeting based on what’s reasonable and appropriate.
Defining Reasonable & Appropriate

- The size and complexity and capabilities of the covered entity
- The covered entity's technical infrastructure, hardware, and software security capabilities
- Sensitivity of the data
- The costs of security measures
- The probability and criticality of potential risks to ePHI

Options for Addressable Specifications

- Implement the specification
- Implement one or more alternative security measures
- Do not implement either an addressable implementation specification or an alternative
- Document your decision!

Administrative Safeguards are defined as...

“Actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures... and manage the conduct of the covered entity’s workforce.”
Administrative Safeguards

Security Management Process
- Risk Analysis (R)
- Risk Management (R)
- Sanction Policy (R)
- Information System Activity Review (R)

Assigned Security Responsibility
- (no spec) (R)

Risk Analysis is the first and possibly the single most important component of your HIPAA Security Compliance Program

Risk Analysis “form the foundation upon which an entity’s necessary security activities are built.” (68 Fed. Reg. 8346.)

Step One: Risk Analysis

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information”

Risk Analysis Report
Why Security Risk Analysis?

- Improves Awareness
- Justification for “Reasonable and Appropriate” for Addressable Implementation Specifications
- Identify assets, vulnerabilities and controls
- Improved basis for decision making
- Justify Expenditures for Security
- Helps determine personnel access levels

Otherwise you are only guessing…and hoping!

How to Conduct a Security Risk Analysis?

1. NIST
   - SP 800-30 – Guidance on Risk Assessment
   - SP 800-66 – Resource Guide for Implementing HIPAA
   - Audit Protocol – June 2012
   - ONC Guide to Privacy and Security of HIT
   - Myths and Facts (p.11)

Vulnerability Scanning and Vulnerability Management
Does HIPAA require vulnerability scans or pentesting?

- Not explicit in the rules
- However, the risk analysis requirement imposes an obligation to identify and document the risks and vulnerabilities to the CIA of ePHI
- Can you do this without vulnerability scans?
- Every security framework (NIST, HITRUST, ISO, COBIT, etc.) includes vulnerability management

What is a Vulnerability?

- A weakness which could potentially allow a hacker to reduce or compromise the confidentiality, integrity or availability of an information system or network
- Contains three intersecting elements
  - a system susceptibility or flaw
  - attacker access to the flaw
  - attacker capability to exploit the flaw

What is Vulnerability Management?

The practice of identifying, classifying, remediating, and mitigating vulnerabilities in networks and software and is often an essential part of security management programs
What is a Vulnerability Scanner

- A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses
- They can be run either as part of vulnerability management process by those tasked with protecting systems – or hackers looking to gain unauthorized access

Types of Scans

- Network Scanners – Deployed on a network and scans end-points as well as network infrastructure
  - Technical expertise required
  - Deployment of Linux machine
  - Most comprehensive
- End-point Scanners
  - Deployed as an “agent” on a client device
  - Easy to deploy
  - Has limited “data discovery” capabilities
- Web-app Scanners
  - Specifically designed for scanning web applications

Vulnerability Assessment Tools

<table>
<thead>
<tr>
<th>Network</th>
<th>End-point Scans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus – Original Open Source tool that became commercial</td>
<td>Healthicity End-point scan tool</td>
</tr>
<tr>
<td>Rapid 7 Nexpose - commercial</td>
<td>Web-app Scanner</td>
</tr>
<tr>
<td>Qualys – commercial</td>
<td>Burp-suite</td>
</tr>
<tr>
<td>OpenVAS – Open Source</td>
<td></td>
</tr>
</tbody>
</table>

8
What is the National Vulnerability Database?

• A Federal Government repository of known vulnerabilities
• They are “scored” using the Common Vulnerability Scoring System (CVSS)
• Scored on a scale of 1 to 10
• Metrics used for score include: exploitability, vector, difficulty, authentication, impact metric based on CIA

Vulnerability Key Considerations

• Report on remediation but does not fix or apply patches
• The objective is to determine the vulnerabilities and report them to the client.
• Must be authorized by the client prior to the performance to protect the assessor from liability
• High False Positive rate
Penetration Testing

Definition of Penetration Testing

• A penetration test evaluates the strengths of security controls on a computer system and network including administrative, physical, operational and technological controls
• A methodical authorized attack on a computer system that looks for security weaknesses and attempts to exploit those weakness in order to "compromise" the CIA of data

Penetration Testing Viewpoints

External vs. Internal
• Can be performed from the viewpoint of an external attacker or a malicious employee

Overt vs. Covert
• Can be performed with or without the knowledge of the IT department of the company being tested

White Box vs Black Box
• Can be performed starting with background and system information or no more information than company name
White Gray and Black Box Testing

• Black Box does not include any knowledge of the structure of the system (simulates the approach of an outside attacker)
• Gray Box includes only a limited knowledge of the layout of the target.
• White Box testing occurs when a penetration tester has significant knowledge of the layout of the target(s) and can make inquiries when needed

Penetration Testing…

• Includes the actual exploitation of the vulnerabilities that are discovered during the phases of the vulnerability assessment
• Includes vulnerability assessment; however, vulnerability assessment does not include penetration testing
• Rules of engagement (ROE) – Agreed to limits on the testers such as off-limit targets or rules that establish when a pen test must be halted
• Must be authorized by the client

Social Engineering Assessment

Social Engineering is a method of attack in which a party uses social techniques and psychological manipulation in order to get the target to performing actions or divulge confidential information. A type of “con” often used for the purpose of information gathering, fraud, or system access
• Pen testers will often use common social engineering techniques to attempt to extract information in order to meet the goals of the engagement
Social Engineering Techniques

- Phishing - a form of deception in which an attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channel
- Spear phishing - an e-mail spoofing fraud attempt that targets a specific organization or person in order to access confidential data. A highly targeted form of attack
- Pre-texting – an elaborate ruse involving a created scenario or impersonation of a person in authority to receive information or payment
- Baiting – Leaving malware infected media such as flash drives in the vicinity of targets and, when used, compromises the network
- Tailgating – following closely behind someone in order to compromise

Goals of Penetration Testing

- Determine feasibility of a particular set of attack vectors
- Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
- Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
- Test the ability of network defenders to detect and respond to attacks
- Provide evidence to support increased investments in security personnel and technology

Phases of Penetration Testing

- Kick-Off
- Discover
- Enumerate
- Verify
- Evaluate
- Report
Kick-off and Discover

**Kick-Off**
- Confirm the scope and parameters of the project with Client the parameters of the assessment.

**Discover**
- Perform reconnaissance activities to identify the Client’s Internet presence
- Use publicly available information
- May include domain names, network segments, and IP addresses
- Network map
- Identify all the hosts within the target environment

Network Enumeration and Scanning

**Purpose**
To discover existing networks owned by a target as well as live hosts and services running on those hosts.

**Methods:**
- Scanning programs that identify live hosts, open ports, services, and other info (Nmap, autoscan)
- DNS Querying
- Route analysis (traceroute)

Enumerate

**Enumerate**
- Vulnerability scanning against the Client’s hosts and web applications
- Enumerate specific host configurations and settings (e.g. running services, the version of the services and operating systems, the purpose of the host, etc.) Use commercial and open source tools to conduct vulnerability scans
- Purpose is to identify all the potential security vulnerabilities
NMap Results

nmap -sS 127.0.0.1
1
2
3 Starting Nmap 4.01 at 2006-07-06 17:23 BST
4 Interesting ports on chaos (127.0.0.1):
5 (The 1668 ports scanned but not shown below are in
6 state: closed)
7 PORT   STATE  SERVICE
8 21/tcp  open  ftp
9 22/tcp  open  ssh
10 631/tcp open  ipp
11 6000/tcp open  X11
12 Nmap finished: 1 IP address (1 host up) scanned in 0.207
13 seconds

WHOIS Results for www.clemson.edu

Domain Name: CLEMSON.EDU
Registrant: Clemson University
340 Computer Ct
Anderson, SC 29625
UNITED STATES
Administrative Contact:
Network Operations Center
Clemson University
340 Computer Court
Anderson, SC 29625
UNITED STATES
(864) 247-5381
hubcap@clemson.edu
Technical Contact:
Mike S. Marshall

DNS Admin:
Clemson University
Clemson University
340 Computer Court
Anderson, SC 29625
UNITED STATES
(864) 247-5381
hubcap@clemson.edu
Name Servers:
EXTNS1.CLEMSON.EDU 130.127.255.252
EXTNS2.CLEMSON.EDU 130.127.255.253
EXTNS3.CLEMSON.EDU 192.42.3.5

Verify

• Review potential vulnerabilities
• Verify the vulnerabilities are not false-positives
• Use penetration techniques and security tools to exploit the vulnerabilities (with a focus on achieving engagement goals and high risks vulnerabilities
• Vulnerability matrix created and updated as exploitable high risk vulnerabilities are discovered during the exploitation process
• Objective is to validate the presence of exploitable security vulnerabilities
Evaluate

- Evaluate the security impact of vulnerabilities and identify solutions to correct them
- Prioritize vulnerabilities based on the impact to and level of effort to remediate
- Develop action plan for remediation
- The goal is to assess the affects of the vulnerabilities to the Client’s security posture.

Report

- Results are documented in a Penetration Assessment Report
- The report will describe:
  - The work performed
  - Security vulnerabilities discovered
  - Recommendations to improve network security
- Includes:
  - The technical details of the findings
  - An executive summary
  - Ranked list of the most significant issues identified
  - Remediation recommendations

Questions?

www.healthcity.com/compliance
support@healthcity.com