PCI/DSS and Vuls
～VulsとPCI/DSS～

許　先明
HEO SeonMeyong

Who am I ?

- Former Provider network engineer (@’95〜’99)
  - ISPのNetwork技術者
- Former network consultant (@’97〜’01)
  - Network設計等のコンサルタント
- Former Server engineer (@’98〜’10)
  - サーバー技術者
- Former JNUG head of the secretariat
  - JNUG(Japan NetBSD Users Group)の元事務局長
- Former Security service manager (@’07〜’11)
  - セキュリティサービスの管理者
- Former Cloud service manager (@’10〜13)
  - クラウドプラットフォームサービスの管理者
- Now Whole infrastructure engineer and consultant (@’13〜)
  - インフラ全般の技術者兼コンサルタント

時間がないので
いきなり本題

- Main Contents -

What is PCI/DSS?

- Payment Card Industry / Data Security Standards
  - クレジットカード業界のセキュリティ基準
- The purpose (目的)
  - Handling the card holder data safety
    - クレジットカード会員データを安全に取り扱う事
- The Formulator (規格策定者)
  - PCI SSC (Security Standards Council)
    - Investors: The five international credit card brand. (VISA/Master/Amex/JCB/Discover)

PCI/DSSとクレカ

- PCI/DSSって美味しいの？
  - 全然美味しくありませんが、従わないとカード決済できなくなるかも
- だれがPCI/DSSに準拠しなければならないの？
  - クレカ情報をInternet経由で取り扱う(やりとりする)人
- クレカ情報ってなに？
  - アカウント情報
    - カード会員データ
      - プライマリアカウント番号 、カード会員名、有効期限、サービスコード
    - 機密情報
      - 全トラックデータ(磁気ストライプ データまたはチップ上の同等データ) 、CAV2/CVC2/CVV2/CID、PINまたはPINブロック

PCI/DSS and Credit Card(CC)

- PCI/DSS is the BEST ?
  - I think the answer is “NO”.
  - You must conform to it while providing a CC settlement service.
- Who must conform to PCI/DSS ?
  - Operators to exchange CC information via the Internet
- What is the CC Information ?
  - Account Informations
    - Cardholder Data
      - Primary Account Number(PAN), Cardholder name, Expiration Date, Service Code
    - Sensitive Authentication Data
      - Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks

PCI/DSSの要件

		データ要素	保存の許可	要件 3.4 に従って、保存されたデータを読み取り不能にする
アカウントデータ	カード会員データ	プライマリアカウント番号（PAN）	はい	はい
		カード会員名	はい	いいえ
		サービスコード	はい	いいえ
		有効期限	はい	いいえ
	機密認証データ[2]	全トラックデータ[3]	いいえ	要件 3.2 に従って保存できない
		CAV2/CVC2/CVV2/CID[4]	いいえ	要件 3.2 に従って保存できない
		PIN/PIN ブロック[5]	いいえ	要件 3.2 に従って保存できない

PCI データセキュリティ基準 – 概要

安全なネットワークとシステムの構築と維持	1. カード会員データを保護するために、ファイアウォールをインストールして維持する 2. システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
カード会員データの保護	3. 保存されるカード会員データを保護する 4. オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
脆弱性管理プログラムの維持	5. マルウェアにしてすべてのシステムを保護し、ウィルス対策ソフトウェアを定期的に更新する 6. 安全性の高いシステムとアプリケーションを開発し、保守する
強力なアクセス制御手法の導入	7. カード会員データへのアクセスを、業務上必要な範囲内に制限する 8. システムコンポーネントへのアクセスを識別　認証する 9. カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	10. ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する 11. セキュリティシステムおよびプロセスを定期的にテストする
情報セキュリティポリシーの維持	12. すべての担当者の情報セキュリティに対応するポリシーを維持する

今時、当然といえば当然の要求

PCI データセキュリティ基準 v3.0
要件とセキュリティ基準
より抜粋

Requirement of PCI/DSS

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

From PCI/DSS 3.2
Requirements and Security Assessment Procedures

Vulsとは？

- ものすごく大雑把にいえば
  - あるシステムにおける
  - 導入されているApplicationに存在する
  - Security的観点から見た脆弱性(平たくいえばBUG)を
  - 公開されているCVE情報と合わせて
  - 検出し、整理するためのツール
  - しかもAgent-less(厳密にはsshdをAgentと言えば言えるのかもしれない)

- 同様のツールにOpenVAS(http://www.openvas.org)がある
  - 昔からあるツールなので、カバレッジも広い
  - 脆弱性診断もできる
  - Agentを導入する必要がある

What is Vuls?

- Overview
  - The Vuls is a tool of
    - pickup and organization
      - of existing vulnerabilities (such like BUGs) in Applications
        - running on some system
          - then checking and matching published information like CVE/NVD/...
  - And agent-less.

- OpenVAS(http://www.openvas.org) is in something a similar tool.
  - System checking tool covering widely many platforms and for a long time.
  - Can assess system vulnerability.
  - Need to install an agent.

VulsとPCI/DSS -ポイント-

- VulsはPCI/DSSに準拠「し続ける」ために利用可能(有用)
  - 「**6.** 安全性の高いシステムとアプリケーションを開発し、保守する」
    - 6.1 セキュリティ脆弱性情報の**信頼できる社外提供元**を使って**セキュリティの脆弱性を特定**し、新たに発見されたセキュ リティの脆弱性に**リスクのランクを割り当てるプロセス**を確立する
    - 6.2 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されている。**重要なセキュリティパッチは、リリース後1カ月以内**にインストールする。
    - 6.6 一般公開されているWebアプリケーションで、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが、次のいずれかの方法によって、**既知の攻撃から保護**されていることを確認する
  - ただし、注意すべき点として以下がある
    - 7.1 システムコンポーネントとカード会員データへの**アクセスを**、業務上必要な人に**限定**する
    - 7.2 システムコンポーネントで、**ユーザの必要性に基づいてアクセスが制限**され、特に許可のない場合は「すべてを拒否」に設定された、**アクセス制御システムを確立**する
    - 8.2 **一意のIDを割り当てる**ことに加え 、すべてのユーザを認証するため、 次の方法の少なくとも1つを使用することで、すべてのシステムコンポーネント上での**顧客以外のユーザと管理者の適切なユーザ認証管理を確認**する。
    - 8.5 次のように、**グループ、共有、または汎用のIDやパスワード**、または他の認証方法が**使用されていない**
    - 8.6 その他の認証メカニズムが使用されている(たとえば、物理的または論理的セキュリティトークン、スマートカード、証明書など)これらのメカニ ズムの使用は、以下のように割り当てる必要がある。

Vuls and PCI/DSS -Point-

- Vuls is useful in order to **continue to maintain** compliance with PCI/DSS
  - ***Requirement 6****: Develop and maintain secure systems and applications*
    - **6.1** Establish a process to identify security vulnerabilities, using **reputable outside sources** for security vulnerability information, and **assign a risk ranking** to newly discovered security vulnerabilities.
    - **6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install ***critical security patches within one month of release***.
    - **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are ***protected against known attacks*** by either of the following methods
  - *Pay attention to the following points*
    - ***7.1 Limit access*** to system components and cardholder data to only those individuals whose job requires such access.
    - ***7.2 Establish an access control system(s)*** for systems components that restricts ***access based on a user's*** need to know, and is set to "deny all" unless specifically allowed.
    - **8.2** In addition to ***assigning a unique ID***, ***ensure proper user-authentication management for non-consumer users and administrators on all system components by employing*** at least one of the following methods to authenticate all users
    - **8.5** ***Do not use group, shared, or generic IDs, passwords***, or other authentication methods as follows
    - **8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows

平たく言うと

- 「脆弱性」を素早く発見し、対処しろ (6条)
- 「権限を分離」して「やっていいことしかさせるな」(8条)
- 「認証」「権限付与」「記録」をちゃんとしろと言うこと
  - セキュリティ保護策の基本

Summery of the point

- Requirement 6: Discover system vulnerabilities and fix them.
- Requirement 8: Has to be administrated by authorized members only.

  - Perform ***authentication***, ***authorization***, ***accounting*** correctly.
    - It is the BASIC of measuring security.

じゃ～、どうすれば？ -1-

- 言葉の定義
  - サービスを提供している検査対象を「対象端末」とする
  - 対象システム内でVulsから命令を受けてコマンドを実行するuserを「対象ユーザー」とする
  - Vulsを実行し検査する機器を「Vuls端末」とする
  - Vulsサーバー内でVulsを実行するuserを「vulsユーザー」とする
  - Vulsサーバーに接続できるアカウントを「管理ユーザー」とする

How to? -Preparation-

- Wording
  - Target Node(TN)　: Inspected node which provide services
  - Target User(TU)　: User account in TN which commands from Vuls
  - Vuls Node(VN)　: The node which run Vuls
  - Vuls User(VU)　: User account in VN whom run Vuls
  - Admin User(AU)　: User account which connect to VN

じゃ〜、どうすれば？ -2-

1. 「対象端末」にはVulsから命令を受けコマンドを実行する「対象ユーザー」を作成する
   - この「対象ユーザー」は**特権ユーザーであってはならない**
2. 「Vuls端末」から「対象端末」へは、**sshを用いてのログインを可能に**する
   - パスワード漏洩の可能性があるため、sshでのログインには「**RSA認証**」を用いるものとする
3. RSA認証を用いる場合、「Vuls端末」側に秘密鍵、「対象端末」側に公開鍵を設置する
   - 「対象端末」側に「対象ユーザー」の**RSA秘密鍵を配置してはならない**
4. 「対象端末」内で「対象ユーザー」が実行するコマンドには管理特権が必要な場合がある
   - 管理特権が必要な場合、特権はsudoもしくは同様のコマンドによって割り当てられるべきである
   - sudo等経由で実行できるコマンドは、**Vulsが必要とする最小限のものに制限**されるべきである
5. 「Vuls端末」は、「対象端末」の脆弱性情報を含めた生のデータが記録される
   - 「Vuls端末」にログイン可能なメンバーは「システムの運用権限を持ち、特に許可された者」に限定する
6. Vulsが出力するデータは、**許可のない一般ユーザーが読み書きできてはならない**
7. Vulsによるscan結果を利用する場合、元データは改変すべきではない
8. Vulsの出力するデータを加工した情報をWEBなどで公開する場合、**アクセス権を持つユーザーを限定**し、かつ**アクセス記録が残る**ようにすべきである

How to?

1. Create **TU** on **TN.**
   - TU ***must not be a*** **Privileged user.**
2. TU on TN accept **login** only from VN **with ssh.**
   - TN **only use "RSA Authentication"** to prevent password leaking.
3. Create ssh "Secret key" on VN and put "Public key" on TN.
   - **Must not put ssh secret key** on TN.
4. On some OSs, TN needs Administrative Privileges.
   - Administrative privileges should be assigned with sudo (or similar commands) only when needed.
   - **Restrict** the commands to run with sudo **to the minimum needed for Vuls**.
5. Raw datas which includes vulnerability informations are recorded on VN.
   - The access to VN is restricted to AU with "Operational Authority".
6. **Only permitted users can read or write** raw data outputted by Vuls
7. Raw data Should not be modified.
8. **Record** should be taken of the **restricted users** that created and published from Vuls raw data.

Conclusion

- Vuls is easy and convenient.
  - Vulsは簡単で便利だ
- Vuls can use a part of tools to maintain PCI/DSS Certificate.
  - PCI/DSS要件を満たすための機能の一部として使える
- Be careful if vuls needs root privileges (ex. RHE/CentOS)
  - Root権限が必要なプラットフォームは注意したほうがいい
- Happy Vuls Life and PCI/DSS Certified system operation!