Segurança em Servidores WEB

DIS

10/10/2018

Agenda

- **SELinux**
- **Firewall**
- **IPSet**
- **Fail2ban**
- **FireHOL**
- **Apache**
- **WAF**
- **ModSecurity**
- **WAF-FLE**
- **Identidade Federada**
- **Shibboleth**

SELinux

Apresentação

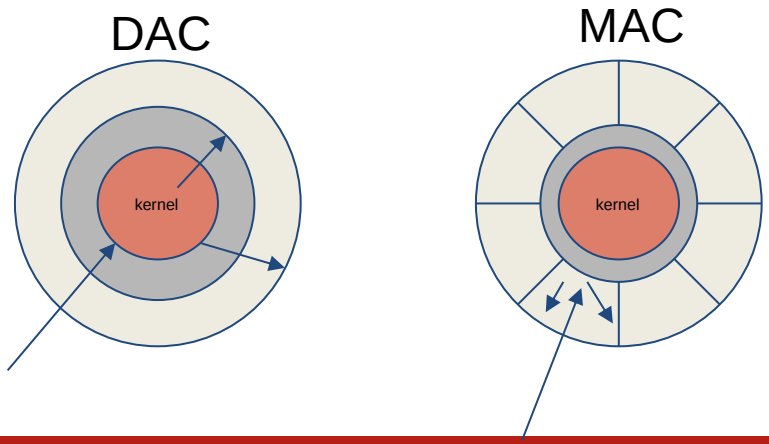
- Site: http://www.selinuxproject.org
- Security Enhanced Linux (SELinux)
- Separação limpa da política da aplicação
- Interfaces de política bem definidas
- Suporte para aplicativos consultando a política e aplicando o controle de acesso (por exemplo, executando tarefas no contexto correto)
- Independência de políticas específicas e linguagens de política
- Independência de formatos e conteúdos específicos de rótulos de segurança
- Rótulos individuais e controles para objetos e serviços do kernel
- Suporte para mudanças de política
- Medidas separadas para proteger a integridade do sistema (tipo de domínio) e a confidencialidade de dados (segurança multinível)
- Política flexível
- Controles sobre inicialização e herança de processos e execução de programas
- Controles sobre sistemas de arquivos, diretórios, arquivos e descritores de arquivos abertos
- Controles sobre soquetes, mensagens e interfaces de rede
- Controles sobre o uso de “recursos”

SELinux

- Informações em cache sobre decisões de acesso através do Cache de Vetor de Acesso (AVC)
- Redução de vulnerabilidades em ataques de escalada de permissões
- Isolamento das aplicações
- Controle de fluxo de informações
- Separação de papéis

Modelos de Controle de Acesso

- Controle de Acesso Discricionário (DAC)
  - Modelo padrão de segurança do Posix
- Controle de Acesso Mandatório (MAC)
  - Modelo padrão de segurança do SELinux



SELinux

Auditoria

- Registros de auditoria no buffer de mensagens do Kernel
- Serviço específico para registros de auditoria - auditd
- Registros do serviço auditd em /var/log/audit.log

Booleanos

- Permite mudança de partes das políticas em tempo de execução
- Pode ser listado pelos comandos semanage e getsebool
- Pode ser definido comando setsebool
- Mais comuns
  - httpd_can_connect_ftp
  - httpd_can_connect_ldap
  - httpd_can_network_connect
  - httpd_can_network_connect_db
  - httpd_can_sendmail
  - httpd_enable_cgi
  - httpd_enable_homedirs

SELinux

Módulos personalizados

- Podem ser instalados, desinstalados, carregados e descarregados em tempo de execução através do comando semodule
- Podem ser criados pelo comando audit2allow
- Podem ser criados reaproveitados em outros equipamentos
- Recomenda-se criar módulos personalizados quando a política padrão não é suficiente para o cenário
- A necessidade de criação pode ser verificada nos logs de auditoria
- A forma mais simples para verificação das necessidades é executar o SELinux em modo permissivo

Firewall

Liberação de portas necessárias

- HTTP e HTTPS (80 e 443)

Ferramentas para bloqueios dinâmicos

- Suporte a bloqueio dinâmico
  - IPSet
- Bloqueios por análises locais
  - Fail2ban
- Bloqueios por análises globais
  - FireHOL

IPSet

Apresentação

- Site: http://ipset.netfilter.org/
- Framework dentro do Kernel do Linux
- Pode armazenar endereços IPs, redes, números de portas TCP/UDP, endereços MAC, nome de interfaces ou combinações de uma certa forma
- Garante velocidade na correspondência de uma entrada contra um conjunto
- Os conjuntos são administrados pelo utilitário ipset
- Recomendável se for necessário
  - armazenar múltiplos endereços IP ou números de porta e corresponder contra a coleção pelo IPTables de uma única vez
  - atualizar dinamicamente regras do IPTables contra endereços IP e números de porta sem penalidade de perda performance
  - expressar conjuntos de regras complexas de endereços IP e portas com uma única regra no IPTables e beneficiar da velocidade de correspondência dos conjuntos do IPSet

Fail2ban

Apresentação

- Site: http://www.fail2ban.org
- Framework IPS que protege o computador de ataques de força bruta
- Escrito em Python
- Capaz de interagir com IPTables e TCP Wrapper
- Varre logs de aplicações e bane IPs que apresentam sinais maliciosos (ex.: múltiplas tentativas de autenticação)
- Possui filtros para diversos serviços
  - Apache
  - Courier
  - SSH
  - entre outros

FireHOL

Apresentação

- Site: https://firehol.org/
- FireHol é uma linguagem (e um programa que a executa)
- É capaz de construir firewalls seguros e orientados a sessão a partir de configuração de fácil entendimento e humanamente legível
- As configurações se mantém legíveis mesmo para ambientes muito complexos
- Ele mantém IP Feeds de Crimes Cibernéticos
  - FireHol IP Feeds: http://iplists.firehol.org/
  - Esse site analisa IP Feeds de segurança disponíveis, principalmente relacionados a ataques online, abuso de serviços online, malwares, botnets, servidores de comando e controle e outras atividades de crimes cibernéticos
  - Esses IP Feeds podem ser utilizados pelo FireHol de forma dinâmica atualizando os ipsets localmente - update-ipsets.sh
  - FireHol IP Sets: https://github.com/firehol/blocklist-ipsets

Apache

Configurações de módulos

- AllowOverride - Tipos de diretivas aceitas nos arquivos .htaccess
  - Recomendável: None
  - Aceitável: AuthConfig (Autenticação/Autorização) / Limit (Controle de acesso de host) / FileInfo (redirecionamento por reescrita e alias, ações e mime)
  - Evitar: All
- AutoIndex - Listagem automática de diretório
  - Recomendável: desabilitar o módulo
  - Aceitável: Options -Indexes (Desabilita a listagem)
- CGI-BIN - Interface para conteúdo dinâmico via chamadas de execução no OS
  - Recomendável: desabilitar o módulo
- UserDir - Diretórios de usuários específicos
  - Recomendável: desabilitar o módulo

Módulos desnecessários

- Recomendável desabilitar

Apache

Métodos de requisição

- **GET** (requisição de conteúdo com passagem de parâmetros por URL)
- **POST** (requisição de conteúdo com passagem de parâmetros pelo corpo HTML)
- **HEAD** (requisição de meta-informações - similar ao GET porém sem corpo HTML)
- **OPTIONS** (retorna os métodos que o servidor suporta para uma determinada URL)

VirtualHosts

- Recomendável definir no virtualhost padrão sem SSL um redirecionamento automático para HTTPS
- Esse redirecionamento pode ser feito de outras formas porém, dessa forma, evita-se que ele seja executada em todas as requisições

Apache

SSL

- Desabilitar Protocolos Inseguros
  - SSL v2/v3
- Desabilitar Cifras Fracas
  - DES
  - 3DES
  - RC4
- Especificar Certificado
- Especificar Chaves
- Especificar Cadeia de Certificação
  - Não apresentar certificado raiz na cadeia - apresentar somente certificados intermediários
- Emissão de Certificados pela DTI / ICP-Edu ou ICPs com Certificados gratuitos
  - Solicitar a DTI pelo canal suporte@dti.ufmg.br
  - ICPs Gratuitos
    - Comodo Certificate Authority - https://ssl.comodo.com/
    - Let's Encrypt - https://letsencrypt.org/
    - SSLForFree - https://www.sslforfree.com/

Apache

Cabeçalhos

- Podem ser definidos pela diretiva Header
- **Content-Security-Policy**
  - Permite que os administradores do site controlem os recursos que o navegador pode carregar para uma determinada página
  - Com algumas exceções, as políticas envolvem principalmente a especificação de origens de servidor e pontos de extremidade de script
  - Ajuda a proteger contra ataques de script entre sites (XSS)
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy
- **Public-Key-Pins**
  - Associa uma chave pública criptográfica específica a um determinado servidor da Web para diminuir o risco de ataques MITM com certificados falsificados
  - Se uma ou várias chaves forem fixadas e nenhuma delas for usada pelo servidor, o navegador não aceitará a resposta como legítima e não a exibirá
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Public-Key-Pins

Apache

- **Referrer-Policy**
  - Rege quais informações do referenciador, enviadas no cabeçalho Referer, devem ser incluídas nas solicitações feitas
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy
- **Strict-Transport-Security**
  - Geralmente abreviado como HSTS, ele permite que um site informe aos navegadores que ele deve ser acessado apenas por HTTPS, em vez de usar HTTP
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
- **X-Content-Type-Options**
  - É um marcador usado pelo servidor para indicar que os tipos MIME anunciados nos cabeçalhos Content-Type não devem ser alterados nem seguidos
  - Isso permite não utilizar o sniffing do tipo MIME ou, em outras palavras, é uma maneira de dizer que os webmasters sabiam o que estavam fazendo
  - Introduzido pela Microsoft no IE 8 como uma maneira dos webmasters bloquearem o sniffing de conteúdo que poderia transformar tipos MIME não-executáveis em tipos MIME executáveis
  - Os testadores de segurança de sites geralmente esperam que esse cabeçalho seja definido
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Apache

- **X-Frame-Options**
  - Pode ser usado para indicar se um navegador deve ou não ser permitido renderizar uma página em um <frame>, <iframe> ou <object>
  - Os sites podem usar isso para evitar ataques de clickjacking, garantindo que o conteúdo deles não seja incorporado a outros sites
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- **X-XSS-Protection**
  - É um recurso do Internet Explorer, Chrome e Safari que impede o carregamento de páginas quando detectam ataques refletidos de cross-site scripting (XSS)
  - Embora essas proteções sejam amplamente desnecessárias em navegadores modernos quando os sites implementam uma forte Política de Segurança de Conteúdo (Content-Security-Policy) que desativa o uso de JavaScript embutido ('inseguro em linha'), eles ainda podem fornecer proteções para usuários de navegadores mais antigos que ainda não suportam o CSP
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Apache

- **Set-Cookie (Aplicação)**
  - Set-Cookie é usado para enviar cookies do servidor para o navegador
  - Esse cabeçalho é definido automaticamente na resposta de acordo com os cookies enviados na requisição e criados/modificados pela aplicação
  - Nas aplicações, é recomendável definir cookies usando opções como httponly, secure e samesite
  - Documentação: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie
- **Ferramenta para teste de cabeçalho**
  - https://www.owasp.org/index.php/OWASP_Secure_Headers_Project

WAF

Apresentação

- **WAF** é um **firewall** para **aplicações HTTP**
- Ele aplica um **conjunto de regras** para uma conversação HTTP
- Cobrem ataques comuns como cross-site scripting (XSS) e SQL injection
- Enquanto **proxies protegem clientes**, **WAFs protegem servidores**
  - Protege uma aplicação WEB específica ou um conjunto delas
- Considerado um proxy reverso
- WAFs podem vir na forma de **appliances**, **plugins** de servidores ou **filtros** e podem ser **personalizados por aplicação**
  - O esforço dessa personalização por aplicação pode ser significante e necessita ser mantido à medida que a aplicação é modificada

Soluções

- **Appliance**
  - Citrix Netscaler Application Firewall
- **Cloud**
  - Amazon Web Services AWS WAF
- **Open-source**
  - ModSecurity

ModSecurity

Apresentação

- Site: https://www.modsecurity.org/
- **Conjunto de ferramentas** para monitoração, registro e **controle de acesso** de **aplicações WEB em tempo real**
- Registro completo do tráfego HTTP
- Avaliação de segurança passiva contínua
- Hardening de aplicativos WEB
- Virtual patching

Modos de execução

- Desligado
- Apenas detecção
- Ligado

Modos de operação

- Traditional
- Anomaly Scoring

ModSecurity

- **Regras**
  - ModSecurity OWASP Core Rule Set (ModSecurity CRS)
    - CentOS 7 - versão 2.2
    - OWASP 3.0
  - **Melhoramentos na CRS3**
    - Redução de 90% de falsos eventos
    - Regras específicas para WordPress e Drupal
    - SQLi/XSS usando libinjection embarcada no ModSecurity

- **Registros de Eventos**
  - Arquivo único (Padrão) - Modo Sequencial
  - Diretórios por data - Modo concorrente
  - mlogc (ModSecurity Log Collector) - Modo remoto
    - */etc/mlogc.conf*
    - */usr/bin/mlogc*

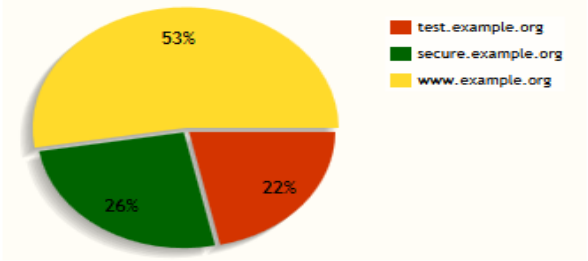
- **Módulos complementares**
  - *mod_unique*

WAF-FLE

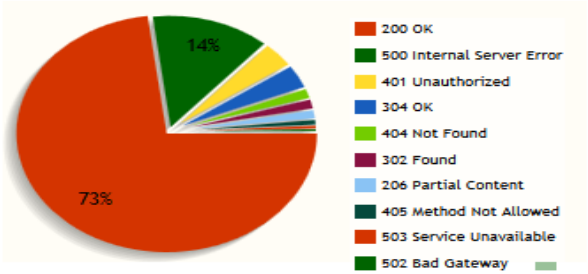
Apresentação

- Site: http://www.waf-fle.org/
- **Console** para visualização de **alertas e relatórios**
- Ambiente LAMP
- **Centralização** de eventos
  - Recebe eventos enviados usando mlog2waffle ou mlogc
- Sem limite da quantidade de sensores
- Filtros
- Download dos eventos no formato original (Raw)
- Wizard para ajudar na configuração

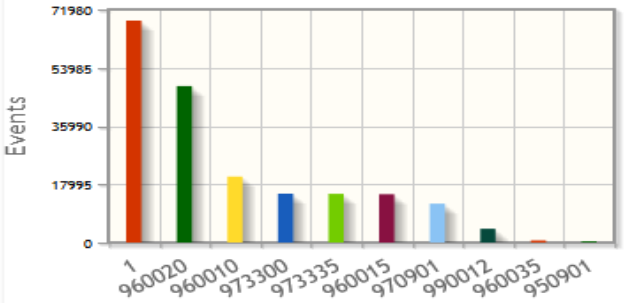
Events per sensor (last 24 hours)



Events per status (last 24 hours)

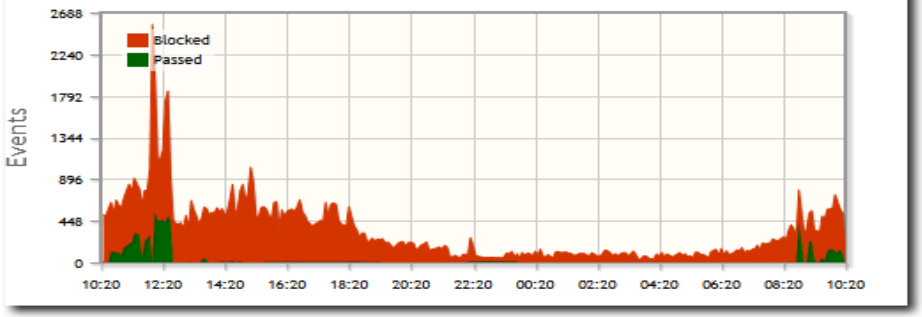


Top Rules in last 24 hours

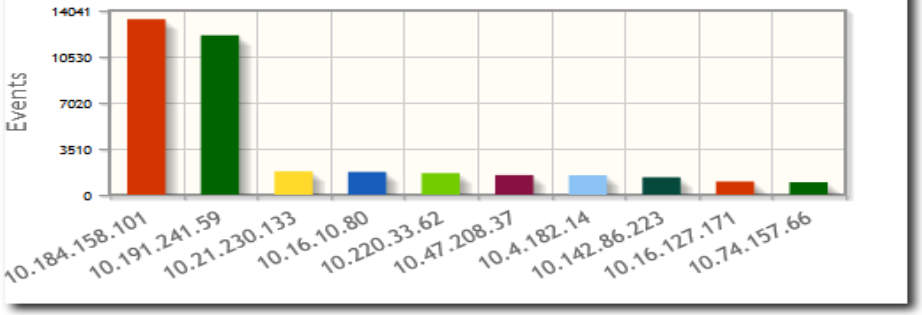


Description:

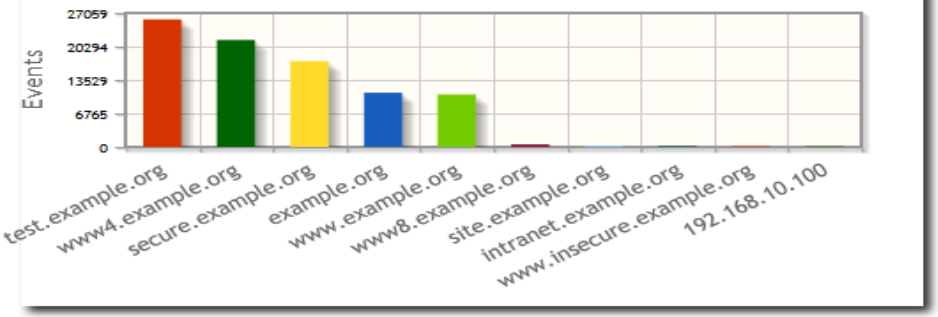
Events in last 24 hours



Top Sources in last 24 hours



Top Targets in last 24 hours



WAF-FLE


WAF-FLE
HOME | EVENTS | FILTER | MANAGEMENT
Logged User: Admin | Logout
Current Filter: [Date: 2011-10-15 00:00:00 Until 2011-10-15 23:59:00 (Reset)] | Clear Filter
Delete
Preserve
1 - 10 of 2026 Next > Last >>
ID Action Sensor Severity Date/Time Source/Port Hostname/Path Rules Alert
207708 teste 2011-10-15 14:35:37 127.0.0.1 58058 Hostname: localhost, Port: 80, Method: GET, Path: /favicon.ico, Protocol: HTTP/1.1, Status Code: 404 (Not Found)
Warning - Sticky SessionID Data Changed - IP Address Mismatch.
Warning - Sticky SessionID Data Changed - User-Agent Mismatch.
Possible Session Hijacking - IP Address and User-Agent Mismatch.
207707 teste 2011-10-15 14:15:03 127.0.0.1 36684 Hostname: localhost, Port: 80, Method: GET, Path: /temporal/, Protocol: HTTP/1.0, Status Code: 404 (Not Found)
Request Missing an Accept Header
Request Indicates a Security Scanner Scanned the Site
Rogue web site crawler (Nikto)
Inbound Anomaly Score (Total Inbound Score: 8, SQLi=, XSS=): Rogue web site crawler
207706 teste 2011-10-15 14:15:03 127.0.0.1 36683 Hostname: localhost, Port: 80, Method: GET, Path: /template/, Protocol: HTTP/1.0, Status Code: 404 (Not Found)
Request Missing an Accept Header
Request Indicates a Security Scanner Scanned the Site
Rogue web site crawler (Nikto)
Inbound Anomaly Score (Total Inbound Score: 8, SQLi=, XSS=): Rogue web site crawler
207702 teste 2011-10-15 14:15:02 127.0.0.1 36679 Hostname: localhost, Port: 80, Method: GET, Path: /system/, Protocol: HTTP/1.0, Status Code: 404 (Not Found)
Request Missing an Accept Header
Request Indicates a Security Scanner Scanned the Site
Rogue web site crawler (Nikto)
Inbound Anomaly Score (Total Inbound Score: 8, SQLi=, XSS=): Rogue web site crawler
207701 teste 2011-10-15 14:15:02 127.0.0.1 36678 Hostname: localhost, Port: 80, Method: GET, Path: /sys/, Protocol: HTTP/1.0, Status Code: 404 (Not Found)
Request Missing an Accept Header
Request Indicates a Security Scanner Scanned the Site
Rogue web site crawler (Nikto)
Inbound Anomaly Score (Total Inbound Score: 8, SQLi=, XSS=): Rogue web site crawler
207700 teste 2011-10-15 14:15:01 127.0.0.1 36677 Hostname: localhost, Port: 80, Method: GET, Path: /swf, Protocol: HTTP/1.0, Status Code: 404 (Not Found)
Request Missing an Accept Header
Request Indicates a Security Scanner Scanned the Site
Rogue web site crawler (Nikto)
Inbound Anomaly Score (Total Inbound Score: 8, SQLi=, XSS=): Rogue web site crawler
207699 teste 2011-10-15 14:15:01 127.0.0.1 36676 Hostname: localhost, Port: 80, Method: GET, Path: /support/, Protocol: HTTP/1.0, Status Code: 404 (Not Found)
Request Missing an Accept Header
Request Indicates a Security Scanner Scanned the Site
Rogue web site crawler (Nikto)
Inbound Anomaly Score (Total Inbound Score: 8, SQLi=, XSS=): Rogue web site crawler
1 - 10 of 2026 Next > Last >>
WAF-FLE, version 0.5.1. Released under GNU General Public License, version 2.

HOME | EVENTS | FILTER | MANAGEMENT

Logged User: Admin | Logout

Delete | Preserve

< Previous 10 of 334 Next >

Rules Match

ID	Severity	Message
960015		Event: Operator EQ matched 0 at REQUEST_HEADERS. Message: Request Missing an Accept Header Tags: | Broken Authentication and Session Management | Failure to restrict URL access | Insufficient Anti-automation
990002		Event: Matched phrase "nikto" at REQUEST_HEADERS:User-Agent. Message: Request Indicates a Security Scanner Scanned the Site Tags: AUTOMATION/SECURITY_SCANNER | Broken Authentication and Session Management | Failure to restrict URL access | Insufficient Anti-automation
990012		Event: Pattern match "(?i:(?:c(?:o(?:n(?:t(?:entsmartz|actbot/)|cealed defense|veracrawler)|mpatible(?: ;(?: msie|\\.)|-)|py(?:rightcheck|guard)|re-project/1.0)|h(?:ina(?: local browse 2\\.|claw)|e(?:rrypicker|esebot))|rescent internet toolpak)|w(?:e(?:b(?: (?:downloader|by ..." at REQUEST_HEADERS:User-Agent. Message: Rogue web site crawler Data: Nikto Tags: AUTOMATION/MALICIOUS | Broken Authentication and Session Management | Failure to restrict URL access | Insufficient Anti-automation
981173		Event: Operator GE matched 4 at TX:restricted_sqli_char_count. Message: Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Data: 7
981176		**Event: Pattern match "(.*)" at TX:960015-PROTOCOL_VIOLATION/MISSING_HEADER-REQUEST_HEADERS. Message: Inbound Anomaly Score Exceeded (Total Score: 26, SQLi=13, XSS=10): Last Matched Message: XSS Attack Detected Data: Last Matched Data: 0**
981204		Event: Operator GE matched 20 at TX:inbound_anomaly_score. Message: Inbound Anomaly Score Exceeded (Total Inbound Score: 26, SQLi=13, XSS=10): XSS Attack Detected

Transaction ID 207303

Sensor	teste
Unique ID	Tpm@@38AAAEAAHhm0woAAAAY
Action	Access denied with code 403 (phase 2)
Score	Total: 26, SQLi: 13, XSS: 10
Source	127.0.0.1 / 54369
Destination	127.0.0.1 / 80
Web App Info	-
Session ID	-
User ID	-
Timestamp	2011-10-15 14:12:28 --0300 (received at 2011-10-15 14:12:28)
Duration	341.035 msec
Server	Apache/2.2.16 (Ubuntu)
Producer	ModSecurity for Apache/2.6.1 (http://www.modsecurity.org/)
Rule Set	core ruleset/2.2.1.

RAW Transaction download

Request Details

HEADER

GET /zorum/index.php?method=<script>alert('Vulnerable')</script> HTTP/1.0
Connection: Keep-Alive
Content-Length: 0
User-Agent: Mozilla/4.75 (Nikto/2.1.1) (Evasions:None) (Test:001454)
Content-Type: application/x-www-form-urlencoded
Host: localhost

Response Details

HEADER

HTTP/1.1 403 Forbidden
Vary: Accept-Encoding
Content-Length: 292
Keep-Alive: timeout=15, max=100
Connection: Keep-Ali
Content-Type: text/html; charset=iso-8859-1

BODY

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /zorum/index.php
on this server.</p>
<hr>
<address>Apache/2.2.16 (Ubuntu) Server at localhost Port 80</address>
</body></html>
```

Identidade Federada

Apresentação

- Uma identidade federada é o meio de vincular a identidade e os atributos eletrônicos de uma pessoa, armazenados em vários sistemas distintos de gerenciamento de identidade
- A identidade federada está relacionada ao logon único (SSO), no qual o tíquete de autenticação única de um usuário, ou token, é confiável em vários sistemas de TI ou mesmo em organizações
- SSO é um subconjunto do gerenciamento de identidade federada e se refere apenas à autenticação e é entendido no nível da interoperabilidade técnica e não seria possível sem algum tipo de federação

Tecnologia

- SAML (Linguagem de marcação para autorização de segurança)
- OAuth
- OpenID
- Tokens de segurança (Tokens da Web simples, Tokens da Web JSON e asserções SAML)
- Especificações de serviços da Web
- Windows Identity Foundation

Identidade Federada

Soluções

- Plataformas de identidade digital
  - Amazon
  - AOL
  - Facebook
  - Foursquare
  - GitHub
  - Google Account
  - LinkedIn
  - Microsoft account – Antigo Windows Live ID
  - MySpace
  - PayPal
  - Twitter
  - Yahoo!

Identidade Federada

Soluções

- Implementações SSO
  - Active Directory Federation Services (Proprietary)
  - CAS (Central Authentication Service) (Free & Open Source)
  - FreeIPA (Free Software)
  - IBM Enterprise Identity Mapping (Proprietary)
  - IBM Tivoli Access Manager (Proprietary)
  - LTPA (Proprietary)
  - Shibboleth (Free & Open Source)
  - Microsoft Account (Proprietary)
  - Ubuntu Single Sign On (Proprietary)

Shibboleth

Apresentação

- Site: https://www.shibboleth.net/
- Projeto da Internet2 Middleware Initiative, que consiste na implementação de padrões amplamente utilizados para autenticação e autorização federada via web
- Utiliza principalmente o SAML (Security Assertion Markup Language) criado pela OASIS (Organization for the Advancement of Structured Information Standards)
- Ele possibilita que o usuário acesse diferentes aplicações web, autenticando-se apenas uma vez (Single Sign-On) em sua instituição de origem

Componentes

- Provedor de Identidade (IdP)
- Provedor de Serviço (SP)
- WAYF (Where Are You From?) / Discovery Service
- Metadados

Shibboleth

Configuração

- **Shibboleth SP**
  - /etc/shibboleth/shibboleth2.xml
    - ID de entidade
    - Definições de sessões
      - Tempo de vida
      - Manipulador SSL
      - Propriedades de cookies
      - Iniciador de sessão
    - Provedor de metadados
      - URI
      - Caminho do arquivo no FS
    - Certificado e chave privada
  - /etc/shibboleth/attribute-map.xml
    - Atributos que serão mapeados pelo SP

- **Configuração do Apache**
  - /etc/httpd/conf.d/shib.conf
    - Contextos que serão protegidos pelo Shibboleth SP

DIS– Divisão de Infraestrutura de Serviços

Perguntas