UNIDADE 2 – SERVIÇOS BÁSICOS DE SEGURANÇA I
MÓDULO 1 – GERENCIAMENTO DE LOGS

01

1 – INTRODUÇÃO

O objetivo deste módulo é a apresentação dos serviços fundamentais para buscar evidências de problemas nos sistemas computacionais em rede. Os conceitos básicos necessários para atingir o mesmo são os que dizem respeito ao gerenciamento de logs, ao sincronismo de tempo e ao monitoramento de serviços.

Serão apresentadas técnicas e tecnologias para o monitoramento de dispositivos e recursos de redes. O aluno terá capacidade para compreender as técnicas e realizar a configuração de ferramentas de sincronismo de tempo, centralização de logs e monitoria de serviços.

Não cabe, nesta disciplina, instruir o estudante em relação à instalação dessas ferramentas. Para isso, é recomendada a consulta aos sites de cada ferramenta. Não vamos realizar as atividades em laboratório, então, cada máquina será um laboratório particular, as ferramentas deverão ser instaladas de acordo com as necessidades de cada um.

ao final de cada módulo você terá exercícios (instalação de Nmap, WinLog, Packet Tracer dentre outros) a serem feitos em sua máquina. Não deixe de fazê-los, pois os exercícios que fará ao longo da unidade cobram conceitos decorrentes das instalações e estudos/pesquisa que fez em sua máquina. Se tiver alguma dificuldade em instalar os programas recorra aos “scripts” mostrados nos módulos, ou então pesquise ou pergunte ao seu coordenador de disciplina. Não deixe para fazê-lo na última hora, pois não dará tempo!

02

Teste seus conhecimentos

Antes de entrar no conteúdo, verifique os seus conhecimentos acerca da segurança de redes, respondendo às questões a seguir. Clique nas respostas para saber se acertou.

1- O que você entende por monitoramento dos recursos de redes?

Resposta 1

2- O que entende por logs?

Resposta 2

Resposta 1:

Monitoramento dos recursos de rede é a verificação do funcionamento de cada serviço e equipamento disponível na rede de computadores.

Resposta 2:

Os logs são uma série de arquivos que são criados e mantidos por uma infraestrutura de software. Estes arquivos contêm a atividade do servidor num passado recente, utilizados pelo administrador do sistema para facilitar o diagnóstico de problemas ou para a verificação do estado do ambiente em determinado momento.

03

2 - GERENCIAMENTO DE LOGS

Estudaremos a partir de agora os seguintes assuntos:

- Gerenciamento centralizado;

- Requisitos de gerenciamento de logs;

- Preservação dos registros em caso de falha do dispositivo;

- Proteção contra sistemas ou usuários mal-intencionados.

2. 1 - Gerenciamento centralizado

O uso de serviços de log centralizados é importante em dois casos principais:

a) para o gerenciamento de falhas nos dispositivos;

b) gerenciamento da segurança com a preservação do registro de eventos em casos de falhas de sistema ou comprometimento de algum dispositivo da rede.

Cada organização possui requisitos diferentes de gerenciamento de logs, que determinarão o detalhamento dos logs coletados, por quanto tempo serão armazenados e como serão analisados.

No gerenciamento de logs, o objetivo é concentrar em um sistema todos os eventos dos equipamentos da rede, *softwares* de segurança, sistemas operacionais e aplicativos.

É necessário concentrar esforços para que esses dados não sejam comprometidos por sistemas mal intencionados. Eles serão úteis na análise de incidentes de segurança ou falhas computacionais. Para isso é necessário que o servidor de logs esteja protegido por um sistema de controle de perímetro, já mencionado anteriormente. Também é necessária a realização de uma configuração segura do servidor, o que será visto adiante.

04

3 - SYSLOG-NG

O syslog-ng é uma ferramenta distribuída com a licença de *software* livre, muito utilizada atualmente. É uma solução que permite a criação de um servidor de logs na rede para vários clientes.

O syslog-ng é uma implementação do protocolo Syslog, definido pela RFC 5424 – The Syslog Protocol. Essa RFC define o protocolo e uma série de particularidades, incluindo a porta padrão do protocolo (UDP 514) e as **facilidades** e **severidades**.

As **facilidades** são categorias que indicam a origem da mensagem. Através delas é possível dispor os registros de log em arquivos separados, organizando melhor as informações.

Com relação às **facilidades** definidas na RFC 5424 – The Syslog Protocol, a tabela a seguir apresenta todas as facilidades definidas na RFC, com seus respectivos códigos e siglas. Como já supracitado, as facilidades são categorias que indicam a **origem da mensagem**. Através delas é possível separar os registros de log em arquivos separados, organizando melhor as informações.

Lista das Facilidades do Syslog-ng (RCF-5424)

Cód.	Nome	Sigla
0	kernel messages	kern
1	user-level messages	user
2	mail system	mail
3	system daemons	daemon
4	security/authorization messages	auth

5	messages generated internally by syslogd	syslog
6	line printer subsystem	lpr
7	network news subsystem	news
8	UUCP subsystem	uucp
9	clock daemon	cron
10	security/authorization messages	authpriv
11	FTP daemon	ftp
12	NTP subsystem	ntp
13	log audit	audit
14	log alert	alert
15	clock daemon	cron
16	local use 0	local 0
17	local use 1	local 1
18	local use 2	local 2
19	local use 3	local 3
20	local use 4	local 4
21	local use 5	local 5
22	local use 6	local 6
23	local use 7	local 7

Fonte: Peixinho, 2013.

Para definir a estratégia de logs, recomenda-se a leitura do artigo Guide to Computer Security Log Management, de Karen Kent e Murugiah Souppaya, do NIST (National Institute of Standarts and Technology).

Além das facilidades, temos as **severidades**, que indicam o nível de "profundidade" do registro de log correspondente.

As severidades definidas no padrão RCF-5424 estão na tabela a seguir.

Lista das Severidades do Syslog-ng (RCF-5424)

Cód.	Nome	Sigla
0	Emergency	emerg
1	Alert	alert
2	Critical	crit
3	Error	err
4	Warning	warning
5	Notice	notice
6	Informational	info
7	Debut	debug

Fonte: Peixinho, 2013

A definição da severidade "0" no sistema significa que apenas as mensagens emergenciais serão registradas. Como a variação do código da severidade é diretamente proporcional à variação do detalhamento do sistema então a quantidade dos registros vai aumentando à medida que a severidade vai variando de "0" até "7". Na severidade "7" todas as ações são registradas. A severidade "7" é útil no auxílio de resolução de problemas, por exemplo, quando um determinado sistema não se comporta como esperado**.**

O syslog-ng é suportado por ambientes heterogêneos, podendo ser configurado em máquinas Linux, BSD e Unix como agente e servidor. Quando o syslog-ng é utilizado como agente ou servidor, é possível que as mensagens sejam transmitidas de forma criptografada na rede.

É possível também sua configuração em sistemas MS Windows, mas somente como agente.

06

O syslog-ng é configurado pela edição do arquivo de configuração "syslog-ng.conf". Definem-se, então, os objetos globais, que são:

Source

É como o syslog-ng vai receber as mensagens. Como agente ele pode receber os logs do sistema do arquivo especial do Unix socks “/dev/log” ou de outras fontes. Exemplo: Unix socks“/dev/log” ou outras fontes.

Destination

É para onde serão enviados ou guardados os logs recebidos pelo syslog-ng. O destino pode ser um arquivo local, um servidor de Syslog na rede ou até mesmo um servidor de banco de dados Oracle, MySQL, Microsoft SQL Server ou outros destinos.

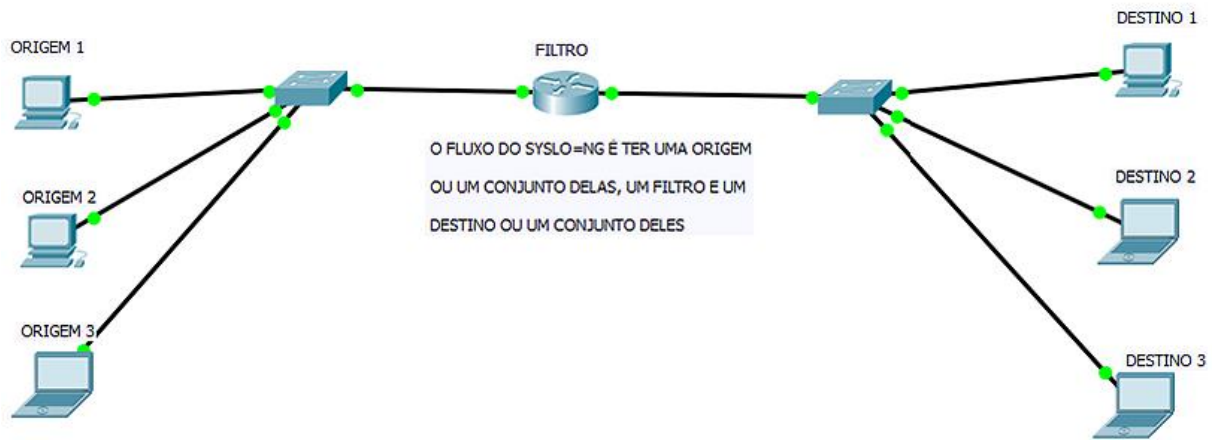
Log Paths

No syslog-ng podem ser definidas várias origens e destinos. O objeto “global log” define o destino de cada origem ou de um conjunto delas.

Filter

Os filtros do syslog-ng incrementam a forma como serão realizados os caminhos dos logs (Syslog-ng como agente e Syslog-ng como servidor). Uma origem ou um grupo de origens não precisa necessariamente ser encaminhado para um destino ou um grupo de destinos, sendo possível filtrar cada tipo de mensagem de origem e com base nesse filtro escolher o destino.

O fluxo do syslog-ng é ter uma origem ou um conjunto delas, um filtro e um destino ou um conjunto deles, conforme ilustra a figura a seguir.



Fluxo syslog-ng
Fonte: O Autor, 2013.

07

3.1 - Syslog-ng como agente

Como dissemos, os filtros do syslog-ng incrementam a forma como serão realizados os caminhos dos logs (Syslog-ng como agente e Syslog-ng como servidor).

Se, por exemplo, um servidor Linux deseja enviar todas as mensagens do sistema e do próprio syslog-ng para um servidor syslog-ng da rede configurada com o endereço IP 10.20.30.2 na porta UDP 514, teremos a seguinte sintaxe para o arquivo de configuração “syslog-ng.conf”:

```
source s_local{unix-stream(“/dev/log”); internal();};

destination d_syslog-server {udp(“10.20.30.2” port(514));};

log{source(s_local); destination(d_syslog-server);};
```

08

3.2 - Syslog-ng como servidor

Neste caso temos a sintaxe do arquivo de configuração do servidor syslog-ng para receber as mensagens dos agentes. Dessa forma, o servidor está configurado para receber as mensagens de syslog na porta UDP 514 e armazenar no arquivo do cliente específico do diretório “/var/log/agente.log”, onde o termo agente será substituído pelo hostname do agente:

```
source s_rede {udp(ip(10.20.30.2 port(514));};

destination d_hosts-file {file(“/var/log/$HOSTS.log“);};

log {source(s_rede); destination(d_hosts-file);};
```

As facilidades podem ser configuradas no syslog-ng através dos filtros, como no exemplo de configuração abaixo:

```
        filter f_cron { facility(cron);};

        log { source(s_local);

        filter (f_cron);

        destination (d_net);};
```

As severidades podem ser configuradas conforme o exemplo abaixo:

```
filter f_debug {level(debug);};

filter f_at_least_info {level(info..emerg);};
```

No exemplo anterior, verifica-se que pode ser criado um filtro contendo mais de uma severidade.

09

Teste seus conhecimentos

Vamos ver se você está entendendo o conteúdo até o momento? Agora, tente responder às questões abaixo, em seguida, clique no link para verificar se você acertou.

1- **Explique os objetivos do gerenciamento de logs.**

Resposta 1

2- **O que é um syslog-ng?**

Resposta 2

Os logs centralizados possibilitam a análise de correlação de logs. Acesse os links citados a seguir.

1) http://www.syslog.org/wiki/Main/LogAnalyzers

2) http://www.ossec.net/

No item a seguir veremos como registrar os logs no sistema operacional Windows.

Resposta1:

Verificação de todos os eventos que ocorrem em um sistema operacional. É um mecanismo utilizado pelos sistemas operacionais, processos e aplicativos que permite o envio de mensagens de atividades e erros, para uma estação de gerenciamento, a fim de se prevenir possíveis ações que podem causar prejuízos à rede de computadores.

Resposta2:

É um servidor de log. SysLog-ng é uma implementação open source do protocolo Syslog para sistemas *nix. Ele filtra com base em conteúdo. Armazena o log de todos os servidores em um único servidor centralizado.

10

4 - Logs do Windows

O padrão Syslog é um padrão Unix, de modo que os sistemas Windows não o utilizam de forma nativa. Dessa forma, não é possível, utilizar apenas os recursos do sistema operacional, redirecionar os registros de log gerados por um sistema Windows para o syslog-ng, como foi feito antes para sistemas Unix. Para minimizar o problema, existem algumas ferramentas que permitem a compatibilidade entre o sistema de logs do Windows e o syslog-ng.

- **WinLogd**

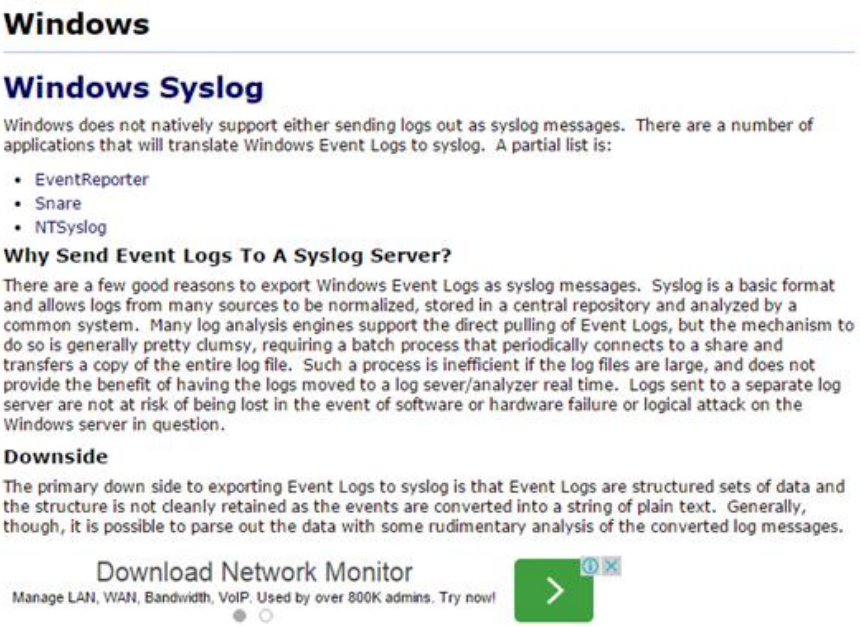
É um sistema capaz de capturar os logs do Microsoft Windows e enviá-los para o sistema de syslog Unix, como o syslog-ng. Uma ferramenta simples e gratuita.

Uma vantagem importante da centralização de logs é a possibilidade de analisar a correlação entre eles, de modo a confrontar logs de diferentes origens e chegar a conclusões interessantes sobre o funcionamento da rede.

O site indicado de analisadores de log é o http://www.syslog.org/. Um desses analisadores de logs, utilizado pela comunidade de segurança, é o OSSEC.

11

Acesse a URL http://www.syslog.org/logged/category/windows/ e siga as instruções abaixo para baixar e configurar o programa.



Windows

Windows Syslog

Windows does not natively support either sending logs out as syslog messages. There are a number of applications that will translate Windows Event Logs to syslog. A partial list is:

- EventReporter
- Snare
- NTSyslog

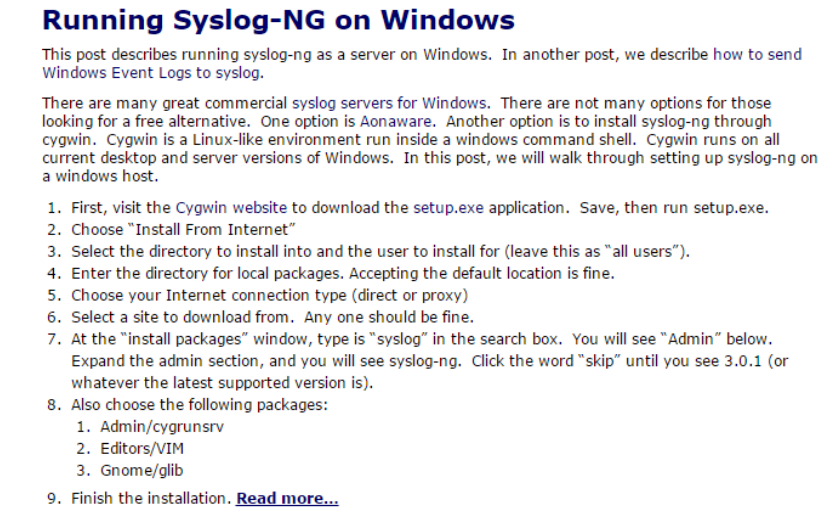
Why Send Event Logs To A Syslog Server?

There are a few good reasons to export Windows Event Logs as syslog messages. Syslog is a basic format and allows logs from many sources to be normalized, stored in a central repository and analyzed by a common system. Many log analysis engines support the direct pulling of Event Logs, but the mechanism to do so is generally pretty clumsy, requiring a batch process that periodically connects to a share and transfers a copy of the entire log file. Such a process is inefficient if the log files are large, and does not provide the benefit of having the logs moved to a log sever/analyzer real time. Logs sent to a separate log server are not at risk of being lost in the event of software or hardware failure or logical attack on the Windows server in question.

Downside

The primary down side to exporting Event Logs to syslog is that Event Logs are structured sets of data and the structure is not cleanly retained as the events are converted into a string of plain text. Generally, though, it is possible to parse out the data with some rudimentary analysis of the converted log messages.

Site para baixar o Windows Syslog
Fonte: www.syslog.org, 2015



Running Syslog-NG on Windows

This post describes running syslog-ng as a server on Windows. In another post, we describe how to send Windows Event Logs to syslog.

There are many great commercial syslog servers for Windows. There are not many options for those looking for a free alternative. One option is Aonaware. Another option is to install syslog-ng through cygwin. Cygwin is a Linux-like environment run inside a windows command shell. Cygwin runs on all current desktop and server versions of Windows. In this post, we will walk through setting up syslog-ng on a windows host.

1. First, visit the Cygwin website to download the setup.exe application. Save, then run setup.exe.
2. Choose "Install From Internet"
3. Select the directory to install into and the user to install for (leave this as "all users").
4. Enter the directory for local packages. Accepting the default location is fine.
5. Choose your Internet connection type (direct or proxy)
6. Select a site to download from. Any one should be fine.
7. At the "install packages" window, type is "syslog" in the search box. You will see "Admin" below. Expand the admin section, and you will see syslog-ng. Click the word "skip" until you see 3.0.1 (or whatever the latest supported version is).
8. Also choose the following packages:
   1. Admin/cygrunsrv
   2. Editors/VIM
   3. Gnome/glib
9. Finish the installation. **Read more...**

Instruções para instalar o Syslog-ng no Windows
Fonte: www.syslog.or, 2015

12

Para a instalação do Winlogd execute as instruções abaixo (podem ocorrer algumas diferenças devido à versão utilizada do Windows):

1. Baixe o winlogd.exe no site indicado e copie para o diretório system32, dentro do diretório de instalação do Windows.

2. Execute winlogd –i para fazer a instalação como um serviço do Windows.

3. Configure o winlogd para enviar os logs para o servidor do syslog-ng, utilizando o registro do Windows (regedit). Os parâmetros são os seguintes (observe que 202 em hexadecimal equivale a 514 em decimal e que o parâmetro Server deve ser alterado para o endereço IP do servidor syslog-ng):

3.1. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\winlogd\ Parameters]

3.2. “Facility”=”local3”

/* string para facilitar a identificação da origem dos logs no servidor central */

3.3. “Port”=dword:00000202

/* porta UDP, que será utilizada para envio dos logs: 514 é a porta padrão do syslog */

3.4. “Server”=”192.168.42.7”

/* endereço do servidor/local para aonde serão enviados os logs */

4. Inicie o serviço com o comando net start winlogd.

5. Configure o syslog-ng para receber os logs. Exemplo de configuração:

source s_net { udp(ip(192.168.42.2) port(514)); };

filter f_winlogd { facility(local3); };

destination d_winlogd { file(“/var/log/winlogd”); };

log { source(s_net); filter(f_winlogd); destination(d_winlogd); }

Qualquer mudança de configuração no winlogd para se tornar efetiva deve ser precedida do reinício do serviço, que pode ser feito com os seguintes comandos:

net stop winlogd

net start winlogd

A seguir veremos alguns servidores úteis na área de segurança, pois é dada pouca atenção a eles, porém são de extrema importância. Eles se referem à hora do servidor ou cliente (aquele relógio analógico ou digital que fica na parte inferior da barra de ferramentas do Windows). Alguns desses plug-ins NTP úteis são: 1) NTP e 2) NetTime.

13

NTP (Network Time Protocol) ou Protocolo de Tempo para Redes, é o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos a partir de referências de tempo confiáveis.

Site do NTP
Fonte: www.ntp.br, 2015.

O NTP pode ser configurado como servidor ou cliente. É um protocolo para sincronização dos relógios dos computadores, baseado em uma fonte confiável: os relógios atômicos do Observatório Nacional, que definem a hora legal brasileira. (para saber mais, consulte: http://ntp.br/).

Veja na figura acima que ele verifica a hora de seu computador e diz se está certa ou errada. A hora da figura corresponde o momento em que a tela no ntp.br foi capturada (a máquina está com a configuração: time-b.nist.gov [clique no relógio abaixo à direita -> alterar configurações de data e hora... -> abra a aba “horário na Internet” -> alterar configurações -> selecionar “Sincronizar com um servidor de horário na Internet” -> escolher “time-b.nist.gov”]).

14

O site armazena o projeto NTP, que desenvolve uma ferramenta de sincronização de relógios para computadores Linux, Unix, VMS e Windows. O NTP pode ser configurado como servidor, como cliente e/ou as duas funcionalidades ao mesmo tempo. Assim, pode-se buscar uma fonte de relógio externa, se assim desejar, e redistribuir essa fonte de hora confiável para a configuração dos relógios das máquinas da rede interna.

A configuração do NTP ocorre com a edição do arquivo ntp.conf, localizado normalmente em /etc/ntp.conf nos servidores Unix. Segue um exemplo de configuração do NTP, no caso do Linux, utilizando como referência os relógios do Comitê Gestor da Internet do Brasil (CGI.br):

```
# “memória” para o escorregamento de frequência do micro
# pode ser necessário criar esse arquivo manualmente com
# o comando touch ntp.drift
driftfile /etc/ntp.drift
# estatísticas do ntp que permitem verificar o histórico
# de funcionamento e gerar gráficos
statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
# servidores públicos do projeto ntp.br
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
# outros servidores
# server outro-servidor.dominio.br iburst
# configurações de restrição de acesso
restrict default kod notrap nomodify nopeer
```

15

Para iniciar o NTP pela primeira vez, utilize o comando:

ntpd –q –g

Dessa forma, o NTP será forçado a sincronizar o relógio local da máquina, mesmo que ele esteja com diferença superior a 16 minutos do servidor NTP da rede. Após iniciar o NTP, você pode deixá-lo rodando na máquina como deamon, com o comando a seguir:

ntpd

Para consultar o estado do aplicativo NTP, utilize o seguinte comando:

ntpq -c pe

Um exemplo de saída do comando acima pode ser vista abaixo:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
***b.ntp.br**	200.20.186.76	2	u	-	64	1	34.838	-32.439	29.778
c.ntp.br	200.20.186.76	2	u	1	64	1	9.252	-33.407	4.105

A saída do comando inclui as seguintes informações:

1) remote;
2) refid;
3) st;
4) when;
5) reach;
6) delay;
7) offset;
8) jitter.

Remote

Nome ou IP da fonte de tempo.

Refid

Identificação da referência (par do sistema) a qual o servidor de tempo remoto está sincronizado.

st

O estado da fonte de tempo.

when

Quantos segundos se passaram desde a última consulta a essa fonte de tempo.

Poll

Intervalo em segundos de cada consulta a essa fonte.

Reach

Registrador de 8 bits, que vai variando do LSb ao MSb, representado na forma octal (cada número representado por 3 bits), que mostra o resultado das últimas 8 consultas à fonte de tempo. Por exemplo: 377 = 11.111.111 significa que todas as consultas foram bem-sucedidas; outros números indica falhas; 375 = 11.111.101, por exemplo, indica que a penúltima consulta falhou.

Delay

Tempo de ida e volta, em milissegundos, dos pacotes até essa fonte de tempo.

Offset

Deslocamento, ou quanto o relógio local tem de ser adiantado ou atrasado (em milissegundos) para ficar igual ao da fonte de tempo.

Jitter

A variação, em milissegundos, entre as diferentes medidas de deslocamento para essa fonte de tempo.

16

O **NetTime** é o protocolo cliente Simple Network Time Protocol (SNTP) para Windows 95/98/Me/NT/2000/XP/Vista/7/8 e servidores 2003/2008/2012. (são suportados por sistemas operacionais de 32 bits e de 64 bits).

Tem os atributos de:

a) ser livre (free);

b) código aberto (open source);

c) ser pequeno (small);

d) fácil de instalar e usar;

e) e o mais importante é que é confiável.

O **NetTime** pode ser obtido na URL http://www.timesynctool.com/

17

Teste seus conhecimentos

Que tal verificar se você está preparado para seguir adiante nos estudos? Responda às questões abaixo e clique na resposta para conferir se você acertou.

1- Como funciona o log no Windows?

Resposta 1

2- O que é um NTP?

Resposta 2

No próximo módulo veremos o monitoramento de serviços e respectivas ferramentas.

Resposta 1

Os logs de eventos no são arquivos especiais que registram eventos importantes no computador (por exemplo, quando um usuário faz logon ou quando um programa encontra um erro). Sempre que esses tipos de eventos ocorrem, o Windows registra o evento em um log de eventos que pode ser lido com o recurso Visualizador de Eventos. Os detalhes nos logs de eventos podem ser úteis para usuários avançados que precisem solucionar problemas com o Windows e outros programas.

Resposta 2

NTP (Network Time Protocol) ou Protocolo de Tempo para Redes é o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos à partir de referências de tempo confiáveis.

18

RESUMO

Com relação ao gerenciamento de logs os principais conceitos são: Gerenciamento centralizado, Requisitos de gerenciamento de logs, Preservação dos registros em caso de falha do dispositivo e a Proteção contra sistemas ou usuários mal intencionados

No gerenciamento de logs, o objetivo é concentrar em um sistema todos os eventos dos equipamentos da rede, softwares de segurança, sistemas operacionais e aplicativos.

O syslog-ng é uma ferramenta distribuída com a licença de software livre, muito utilizada atualmente. É uma solução que permite a criação de um servidor de logs na rede para vários clientes. O padrão que norteia o syslog-ng é o RFC 5424 – The Syslog Protocol. O syslog-ng é suportado por ambientes heterogêneos, podendo ser configurado em máquinas Linux, BSD e Unix como agente e servidor. É possível também sua configuração em sistemas MS Windows, mas somente como agente.

O WinLogd é um sistema capaz de capturar os logs do Microsoft Windows e enviá-los para o sistema de syslog Unix, como o syslog-ng. Uma ferramenta simples e gratuita.

Não se esquecer dos servidores úteis na área de segurança, pois é dada pouca atenção a eles, porém são de extrema importância. Eles se referem à hora do servidor ou cliente (aquele relógio analógico ou digital que fica na parte inferior da barra de ferramentas do Windows). Alguns desses plug-ins NTP úteis são: 1) NTP e 2) NetTime.

NTP (Network Time Protocol) ou Protocolo de Tempo para Redes é o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos a partir de referências de tempo confiáveis.

O NetTime é o protocolo cliente Simple Network Time Protocol (SNTP) para Windows 95/98/Me/NT/2000/XP/Vista/7/8 e servidores 2003/2008/2012 (são suportados por sistemas operacionais de 32 bits e de 64 bits).

UNIDADE 2 – SERVIÇOS BÁSICOS DE SEGURANÇA I
MÓDULO 2 – MONITORAMENTO DE SERVIÇOS E AVALIAÇÃO DE FERRAMENTAS

01

1 – FERRAMENTAS DE MONITORAMENTO DE SERVIÇOS

As ferramentas de monitoramento são um subconjunto do universo de ferramentas de gerenciamento focadas na obtenção de informações sobre elementos de infraestrutura de TI.

Entre as ferramentas de monitoramento, destacamos algumas com o código-fonte aberto e distribuído sob a licença GNU GPL.

A seguir são citadas as principais ferramentas que deverão ser baixadas e testadas nas máquinas de cada um de vocês para que tenham uma visão geral das funcionalidades e potencialidades de cada uma. Veremos, portanto, as seguintes ferramentas:

- Nagios,
- Zabbix,
- Cacti,
- Ntop.

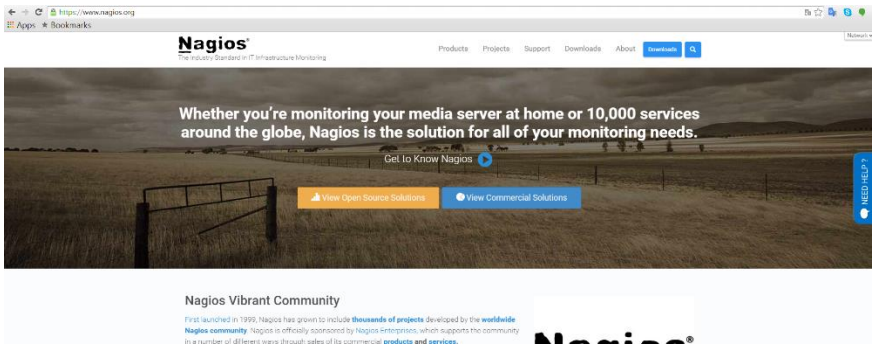
A ideia é que manipulem e familiarizem-se com as mesmas, uma vez que não temos laboratório físico para montarmos nossos servidores e clientes distintamente.

02

1.1 - Nagios

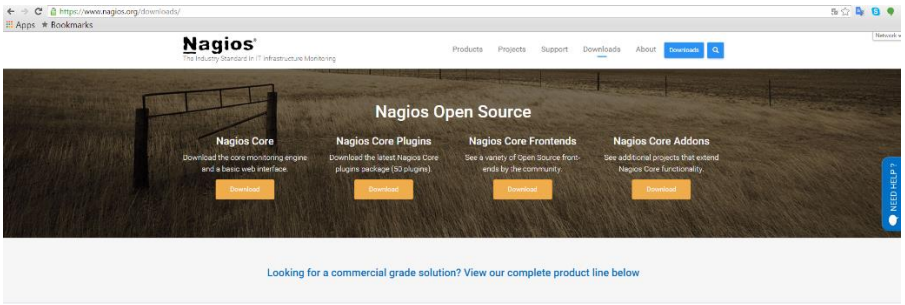
O Nagios é uma ferramenta de gerenciamento que monitora os elementos e serviços de rede.

Pode ser obtido no endereço https://www.nagios.org/ conforme figura abaixo.



Site para obtenção do Nagios
Fonte: www.nagios.org, 2015

Na seção de *downloads* você tem as opções a seguir:



Site para downloads do Nagios.
Fonte: www.nagios.org, 2015.

03

No Brasil temos a comunidade Nagios, conforme a figura abaixo. Verifique na URL http://nagios.br.com.

Site do Nagios.br.com
Fonte: www.nagios.br.com, 2015.

Ele permite que você faça um gerenciamento da infraestrutura de TI de sua instituição.

04

Os dados são coletados através de testes que simulam o funcionamento de aplicações como:

- File Transfer Protocol (FTP);
- Secure Shell (SSH);
- Hypertext Transfer Protocol (HTTP);
- Simple Mail Transfer Protocol (SMTP);
- Post Office Protocol version 3 (POP3);
- Network Time Protocol (NTP);
- Internet Control Message Protocol (ICMP);

Ou através de plugins adicionais que podem ser desenvolvidos e integrados ao Nagios.

Site do Nagios
Fonte: www.nagios.br.com, 2015.

A figura, acima, mostra as possibilidades do Nagios, na qual se pode ter uma visão abrangente do estado dos servidores que estão sendo monitorados pela ferramenta.

05

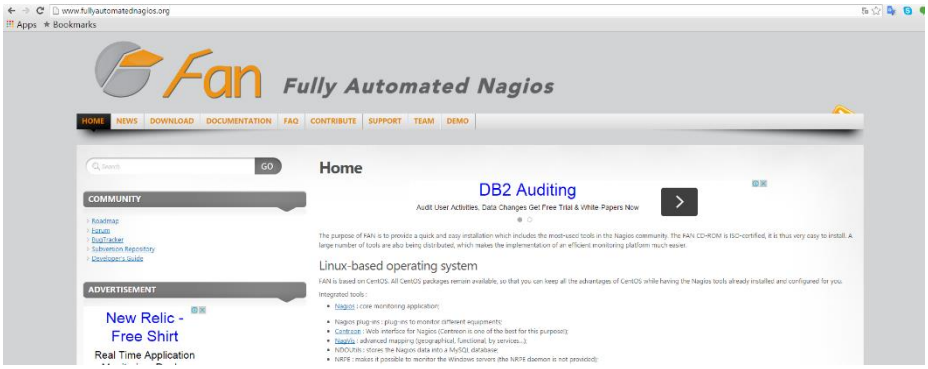
Diversos plugins estão disponíveis na internet e podem ser utilizados pelo administrador para testes mais completos. A interatividade com o administrador baseia-se no envio de mensagem eletrônica, alerta no console e mensagem SMS para celulares sobre o problema ocorrido.

O grande destaque dessa ferramenta é a possibilidade de classificação de grupos de usuários para receber relatórios e alertas do sistema. Por exemplo, o problema de um determinado servidor pode ser comunicado ao responsável pelo serviço, bem como para uma equipe responsável pelos equipamentos ou ativos de rede.

Toda a sua configuração é realizada em arquivos de texto, e a interface com o usuário é realizada em um console web. É possível obter relatórios de disponibilidade e planejar ações corretivas para os problemas ocorridos em equipamentos da rede.

Existe ainda o projeto Fully Automated Nagios (FAN), que tem por objetivo prover uma instalação facilitada do Nagios e ferramentas auxiliares providas pela comunidade. O projeto FAN disponibiliza inclusive uma imagem em CD-ROM (ISO), que facilita a instalação de um servidor Nagios.

Observe a figura a seguir.



Site do FAN.
Fonte: www.fullyautomatednagios.org, 2015.

Fully Automated Nagios

O FAN - Fully Automated Nagios - pode ser obtido no endereço http://www.fullyautomatednagios.org/

06

1.2 - Zabbix

O Zabbix é uma ferramenta de gerenciamento que monitora os elementos e serviços de rede.

Os dados são coletados através de consultas ao SNMP (Simple Network Management Protocol), de ferramentas de testes que simulam o funcionamento das aplicações FTP (File Transfer Protocol), SSH (Secure Shell), HTTP (Hypertext Transfer Protocol) ou através de plugins adicionais que podem ser desenvolvidos e integrados ao Zabbix.

Conforme o site, é o *software* de nível empresarial final projetado para disponibilidade e desempenho de componentes de infraestrutura de TI de monitoramento. Zabbix é *open source* e pode ser obtido sem custos.

Sua funcionalidade de monitoramento em tempo real de alto desempenho significa que dezenas de milhares de servidores, máquinas virtuais e dispositivos de rede podem ser monitorados simultaneamente.

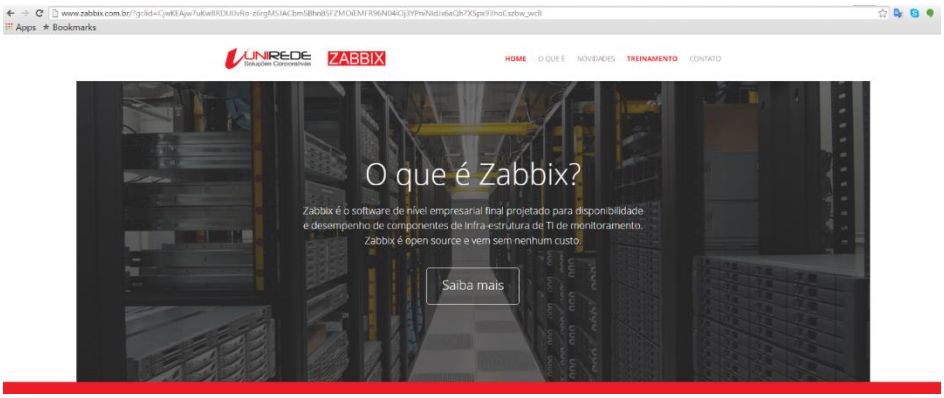
Os dados de armazenamento, os recursos de visualização estão disponíveis por meio de sínteses, mapas, gráficos, telas e outros. Além disso, diversas formas de analisar os dados com a finalidade de alertar estão disponíveis. Limites aceitáveis para os dados de entrada podem ser definidos. Se esses limites forem ultrapassados o Zabbix notifica, por e-mail, informando os administradores de rede sobre o atual ou um problema em potencial.

Site

A ferramenta pode ser obtida no endereço:
http://www.zabbix.com.br/?gclid=CjwKEAjw7uKwBRDUlJvRo-z6rgMSJACbmSBhn8SFZMOiEMFR96N04iOj3YPniNIdJx6aQh7X5px93hoCszbw_wcB

07

Veja figura abaixo.



Site do Zabbix.
Fonte: www.zabbix.com.br, 2015.

Todos os dados coletados pelo Zabbix são armazenados em uma base de dados SQL (Structured Query Language), permitindo a geração de relatórios predefinidos e personalizados, e ainda a utilização de ferramentas especializadas para gerar relatórios. Entre os relatórios padrão gerados pelo Zabbix, temos os relatórios de disponibilidade, de nível de serviços, de tráfego de rede e de utilização de recursos, como CPU (Central Processing Unit) e memória.

Toda a configuração do Zabbix é realizada através de uma interface web limpa e amigável. Os alarmes são emitidos no console web do usuário, via recursos de áudio, mensagens eletrônicas e/ou envio de SMS (Short Message Service) para aparelhos celulares. O Zabbix permite a geração de gráficos on-line e oferece ao administrador a possibilidade de criar mapas personalizados da rede. A seguir imagem de uma tela de monitoramento do Zabbix.

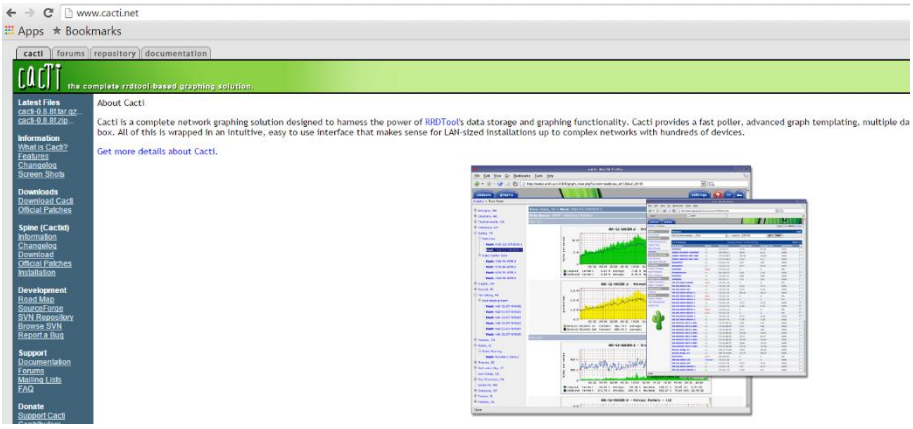
08

1.3 - Cacti

O Cacti é uma ferramenta de monitoração criada por Ian Berry.

Surgiu como uma opção de *frontend* (interface gráfica com o usuário para interagir com programas) que apresenta os gráficos dos dados obtidos através de consultas SNMP ou de scripts. Esses dados são armazenados pelo Round-Robin Database Tool (RRDTool).

O Cacti pode ser obtido no endereço http://www.cacti.net/, conforme figura abaixo.



Site do Cacti
Fonte: www.cacti.net, 2015.

RRDTool

É um software que armazena e mostra dados em série obtidos em um determinado período de tempo.

09

O Cacti disponibiliza um ambiente de configuração e operação agradável e acessível (interface web escrita em PHP), com controle de acesso por nível de usuário. As informações de configuração são armazenadas em um banco de dados SQL. Sua arquitetura prevê a possibilidade de expansão através de plugins, que adicionam novas funcionalidades, tornando-o ainda mais completo.

O Cacti é muito usado em monitoramento de links WAN, por conta da sua facilidade na criação de gráficos para monitorar a banda nos links contratados por operadoras. Apesar dessa funcionalidade importante, o Cacti pode ainda monitorar uma série de parâmetros importantes, como consumo de CPU, memória e espaço em disco, entre outros. A sua capacidade de apresentar os dados de maneira gráfica o torna um excelente complemento para o Nagios na tarefa de monitoramento.

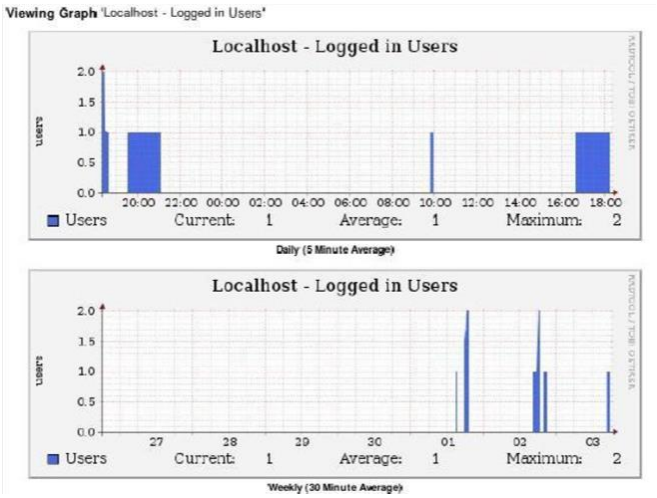


Imagem de monitoramento do Nagios.
Fonte: nagios, 2015.

Existe ainda uma versão facilitada, que oferece uma distribuição Linux com o Cacti pré-instalado. Ela se chama CactiEZ e é uma boa opção para iniciantes que querem começar rapidamente a utilização da ferramenta.

10

1.4 - Ntop

O Network Traffic Probe (Ntop) é uma ferramenta livre para análise de tráfego de rede.

Possui um servidor HTTP (Hypertext Transfer Protocol) e HTTPS (Hypertext Transfer Protocol Secure) nativo, que apresenta uma série de gráficos do tráfego e estatísticas da rede. Possui ainda um modo interativo no console de texto.

Principais **objetivos** do Ntop:

a) Monitoramento e medida do tráfego;

b) Planejamento e personalização da rede;

c) Detecção de violações na segurança.

Com desenvolvimento iniciado em 1998 por Luca Deri, o Ntop opera nas plataformas Unix (incluindo Linux, BSD, Solaris e MacOSX) e Microsoft Windows.

A coleta de informações é feita através da análise do tráfego das informações que passam pelas interfaces da rede local.

Principais **características** do Ntop:

a) Suporte ao Cisco NetFlow/sFlow;

b) Identificação de sub-redes e seus usuários;

c) Suporte ao WAP (Wireless Application Protocol);

d) Ordenação de tráfego.

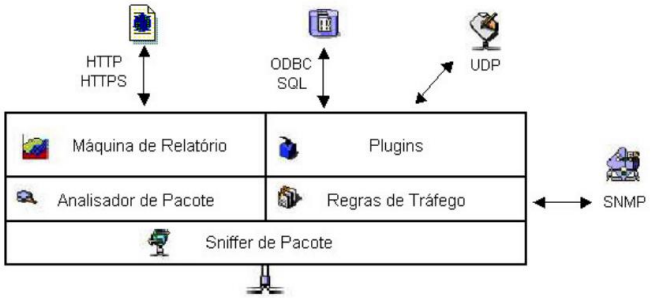
11

A figura seguinte mostra a estrutura funcional do Ntop, seus módulos e os itens que completam a ferramenta:

a) Servidor web (HTPS/HTTPS);

b) Banco de dados (ODBC SQL) e

c) Protocolos (UDP/SNMP).



Estrutura funcional do Ntop
Fonte: Internet, 2015.

Nessa figura:

a) a máquina de relatório é um servidor web;

b) os plugins são resumidos no banco de dados e no protocolo de transporte;

c) o analisador de pacote é o Ntop;

d) as regras de tráfego são as regras do SNMP (Simple Network Management Protocol" ou "Protocolo Simples de gerenciamento de redes");

e) o investigador do pacote é um sniffer qualquer;

f) o cabo Ethernet é a tecnologia de rede que liga máquina que roda o Ntop.

12

2 - AVALIAÇÃO DAS FERRAMENTAS

As ferramentas apresentadas podem ser classificadas em três grupos:

a) de **monitoração de serviços**, como Nagios e Zabbix;

b) **especializadas na geração de gráficos**, como Cacti e Zabbix;

c) de **classificação de tráfego**, como Ntop.

O **Zabbix** é uma ferramenta com algumas características que permitem que ela seja classificada também como ferramenta especializada na geração de gráficos, ainda que estes gráficos possuam menos recursos funcionais que os gráficos do Cacti.

Quase todas as ferramentas mencionadas são fáceis de instalar. A configuração do Nagios é a mais complexa por exigir a manipulação de vários arquivos de texto. As demais ferramentas possuem

interface web para configuração, estando bem documentadas e com vários artigos de referência publicados na internet.

Comparação de características das ferramentas.

Características	Nagios	Zabbix	Cacti	Ntop
Open Source	Sim	Sim	Sim	Sim
Console web	Sim	Sim	Sim	Sim
Administração web	Não	Sim	Sim	Sim
Monitoramento de serviços	Sim	Sim	Via Plugin	Não
Relatórios de disponibilidade	Sim	Sim	Via Plugin	Não
Coleta de dados SNMP	Via Plugin	Sim	Sim	Não
Monitoramento de recursos	Sim	Sim	Sim	Não
Mapas de rede	Sim	Sim	Via Plugin	Tráfego
Classificação do tráfego de rede	Não	Via Plugin	Via Plugin	Sim
Coleta de Network Flows	Não	Não	Não	Sim
Detecção de violações de segurança	Não	Não	Não	Sim

Fonte: Peixinho, 2013.

13

2.1- Vantagens do Cacti

Dentre as opções apresentadas, o Cacti foi escolhido para ser a ferramenta usada nesta disciplina, pelas seguintes razões:

a) Ser simples de usar e adequado para um ambiente de laboratório;

b) Apresentar uma plataforma bem documentada;

c) Possuir um agente eficiente com possibilidade de expansão de características (uso de registros gerados por ferramentas externas);

d) Possuir arquitetura modular, que permite a integração de novos plug-ins;

e) Capacidade de gerar gráficos;

f) Capacidade de coletar informações por consultas SNMP.

Apesar de as atividades práticas deste módulo trabalhar apenas com a ferramenta disponível no Packet Tracer, o aluno está convidado a experimentar as outras ferramentas. As instruções apresentadas neste módulo servem como ponto de partida para que o aluno seja capaz de instalar e configurar qualquer uma das ferramentas apresentadas. Muitas delas possuem versões pré-instaladas, em Live CDs, ou distribuições Linux customizadas de fácil instalação.

Foi visto que um dos aspectos mais importantes de uma rede de computadores é a auditoria para assegurar que tudo está dentro da conformidade, por isso vamos estudar as mensagens de log.

Elas registram tudo que ocorreu nos dispositivos da infraestrutura, desde alterações nas configurações, registro de acessos, falha de protocolos, status das interfaces e outros. No IOS/Cisco as mensagens de log são trazidas na própria tela do console para o administrador (por padrão) e armazenadas apenas em memória interna (*buffer*).

14

Isso não é suficiente para assegurar que posteriormente possam ser realizadas auditorias através da verificação dos logs, então vamos configurar equipamentos da infraestrutura para encaminharem as mensagens de log para uma fonte externa, por exemplo, um servidor de gerenciamento que esteja executando o serviço de syslog.

Existem várias soluções no mercado para esse fim que podem ser pagas ou gratuitas e baseadas nas mais diversas plataformas (Linux, Windows).

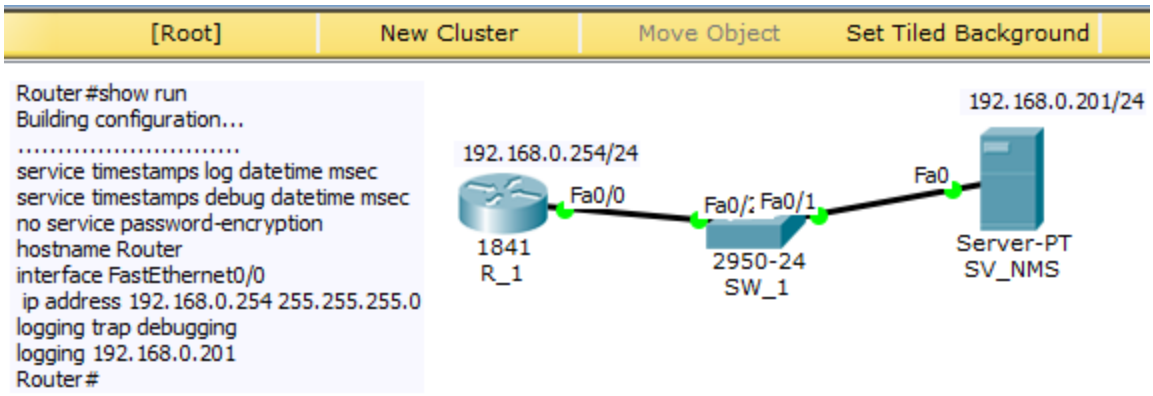
Outra sugestão gratuita baseada em Linux, que o estudante pode instalar em casa para testar o procedimento de configuração do redirecionamento das mensagens de log para um servidor externo via syslog, é o JFFNMS (Just For Fun Network Management Station). Ele é uma solução completa de gestão/ monitoração (*network management station*) que entende os principais protocolos utilizados para fins de monitoramento e controle: SNMP, Syslog e TACACS.

Para aqueles habituados com a instalação manual de aplicativos no Linux, sugerimos baixar o código fonte do aplicativo na página do projeto (http://www.jffnms.org/). Caso você seja usuário Debian/Ubuntu, esse processo pode ser simplificado através do uso dos repositórios tradicionais.

Antes de instalar o JFFNMS, você irá precisar o MySQL e do Apache instalados na máquina, afinal o sistema é todo acessado via web (apache) e as informações monitoradas têm que ser armazenados em algum banco de dados (mysql).

15

Na figura abaixo vocês podem verificar o cenário que será utilizado no exemplo. Trata-se de ambiente bem simples em que temos (i) uma rede local (LAN), (ii) um roteador que iremos configurar para encaminhar as mensagens de log.



Syslog com o Packet Tracer
Fonte: O Autor, 2015.

Clique aqui para visualizar o exercício.

Clique aqui

Produção: inserir como link a figura “Syslog com o Packet Tracer.pkt” anexa ao módulo.

16

O procedimento de configuração do roteador (ou de um switch) para encaminhar todas as mensagens de log (syslog) para um servidor externo é bastante simples e direto, bastando para tal a entrada das seguintes linhas de comando, no caso no roteador R_1:

1. Router>enable

2. Router#configure terminal

3. Router(config)#service timestamps debug datetime msec

4. Router(config)#service timestamps log datetime msec

5. Router(config)#logging 192.168.0.201

6. Router(config)#logging trap debugging

7. Router(config)#end

8. Router# show logging

Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 4 messages logged, xml disabled, filtering disabled

Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled

Buffer logging: disabled, xml disabled, filtering disabled

Logging Exception size (4096 bytes)

Count and timestamp logging messages: disabled

Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

Trap logging: level debugging, 4 message lines logged

Logging to 192.168.0.201 (udp port 514, audit disabled,

authentication disabled, encryption disabled, link up), 2 message lines logged, 0 message lines rate-limited,

0 message lines dropped-by-MD,

xml disabled, sequence number disabled

filtering disabled

```
Router#
```

Nas linhas 3 e 4 roteador anexa a data/hora às mensagens de log, caso contrário não faria muito sentido armazená-las em um servidor externo para realização de auditoria.

Na linha 5 as mensagens de log são direcionadas para o servidor que estará executando o serviço syslog de armazenamento das mensagens e na linha 6 indica-se que os avisos (*warnings*) também deverão ser armazenados no servidor, não apenas mensagens de erro mais severas.

A Cisco trata as mensagens de log em 8 níveis diferentes (de 0 a 7), dependendo da severidade do evento ocorrido. Esses níveis de mensagens de log são:

0 -> Emergência

1 -> Alerta

2 -> Crítico

3 -> Erro

4 -> Aviso

5 -> Notificação

6 -> Informação

7 -> Debug

Por padrão, todas as mensagens de severidade 0 a 3 (emergência, alerta, crítico e erro) são direcionadas para o servidor externo de log porque dizem respeito a eventos graves que comprometem de alguma forma o funcionamento do sistema. Caso o administrador queira armazenar inclusive as mensagens de menor severidade (valores maiores de 4 a 7) ele deve informar explicitamente na configuração.

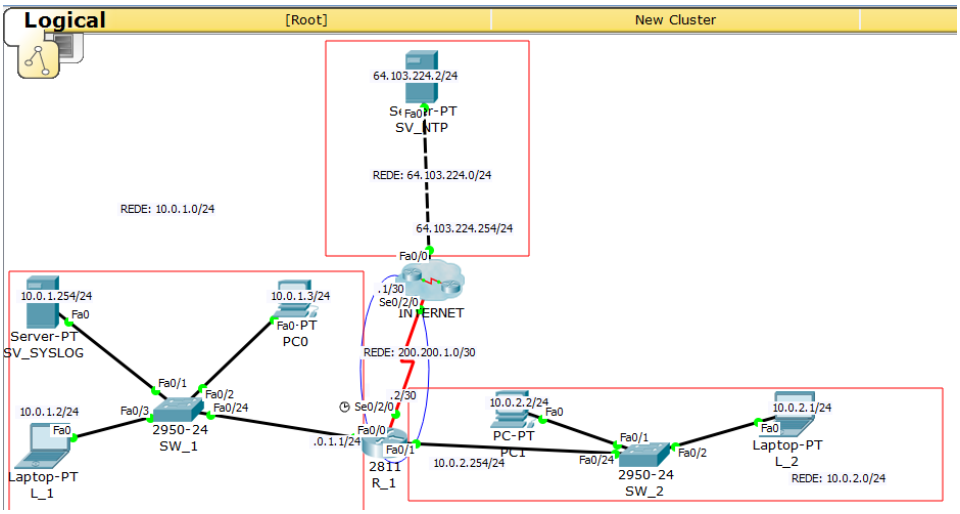
A linha 8 serve para verificar o status do cliente syslog que está em execução no roteador configurado, em que obterá uma saída com o resumo da quantidade de mensagens de log por categoria. Com o roteador configurado e o serviço JFFNMS em execução no servidor (NMS), o resultado é que através da estação de gerenciamento é possível acompanhar as mensagens de log de maneira mais centralizada através da interface web. Bons testes com a ferramenta gratuita!

17

Vamos a mais um exemplo de configuração com o Packet Tracer do SysLog e do NTP (Network Time Protocol).

Seja o cenário abaixo:

Cenário



Configuração do SysLog e do NTP no Packet Tracer
Fonte: O Autor, 2015.

Clique aqui para visualizar o exercício. Neste exercício, você ativará e usará o serviço de syslog (sistema de registro) e o serviço de ntp (network time protocol) de modo que o administrador de rede possa monitorar a rede com mais eficiência.

Parte 1: configurar o serviço syslog

etapa 1: ative o serviço syslog.

a. clique no SV_SYSLOG e, em seguida, na guia services.

b. ative o serviço de syslog e mova a janela, para um lugar que no atrapalhe o seu cenário, para que você possa monitorar a atividade (redimensione as janelas se necessário).

etapa 2: configure os dispositivos intermediários para usarem o serviço syslog.

a. configure R_1 para enviar eventos de log ao servidor SV_SYSLOG:

R1(config)# logging 10.0.1.254

b. configure SW_1 e SW_22 para enviar eventos de log ao servidor SV_SYSLOG:

SW_1(config)#logging 10.0.1.254.

SW_2(config)#logging 10.0.1.254.

c. configure SW_2 para enviar eventos de log para o endereço ip do servidor SV_SYSLOG.

Parte 2: gerar eventos registrados

etapa 1: altere o status das interfaces para criar logs de eventos.

a. configure uma interface de loopback 0 em R_1 e, em seguida, desative-a.

b. desconecte os PC0 e PC1. em seguida, ative-os novamente.

etapa 2: examine os eventos de syslog.

a. consulte os eventos de syslog. observação: todos os eventos foram gravados, no entanto, os

timestamps estão incorretos.

b. cancele o log antes de passar para a próxima fase.

Parte 3: ajustar manualmente relógios dos switches

etapa 1: ajuste manualmente os relógios nos switches SW_1 e SW_2 à data atual e à hora aproximada. Por exemplo:

sw_1# clock set 16:47:00 out 15 2015

etapa 2: ative o serviço de logging de data e hora nos switches.

configure SW_1 e SW_2 para enviar seu timestamp com logs que ele envia ao servidor SV_SYSLOG.

sw_1(config)# service timestamps log datetime msec

Parte 4: configurar o serviço ntp

etapa 1: habilite o serviço ntp. Neste exercício, supomos que o serviço ntp esteja hospedado em um servidor de Internet público. Se o servidor ntp for privado, a autenticação também poderá ser usada.

a. clique em sv_ntp, abra a guia services do servidor ntp.

b. ative o serviço ntp e observe a data e hora exibida.

etapa 2: ajuste automaticamente o relógio automático no roteador em R_1 para a data e hora de acordo com o servidor ntp.

R_1(config)# ntp server 64.103.224.2

etapa 3: ative o serviço de logging de data e hora do roteador.

configure R_1 para enviar seu timestamp com logs que ele envia ao servidor syslog.

Parte 5: verificar os logs de data e hora

etapa 1: altere o status das interfaces para criar logs de eventos.

a. ative novamente e, em seguida, desative a interface de loopback 0 em R_1.

b. desconecte os laptops L_1 e L_2. em seguida, ative-os novamente.

etapa 2: examine os eventos de syslog. Consulte os eventos de syslog. Observação: todos os eventos foram gravados e os timestamps estão corretos como configurados. R_1 usa as configurações do relógio do servidor ntp, e SW_1 e SW_2 usam as definições do relógio configuradas por você na parte 3.

fim do exercício.

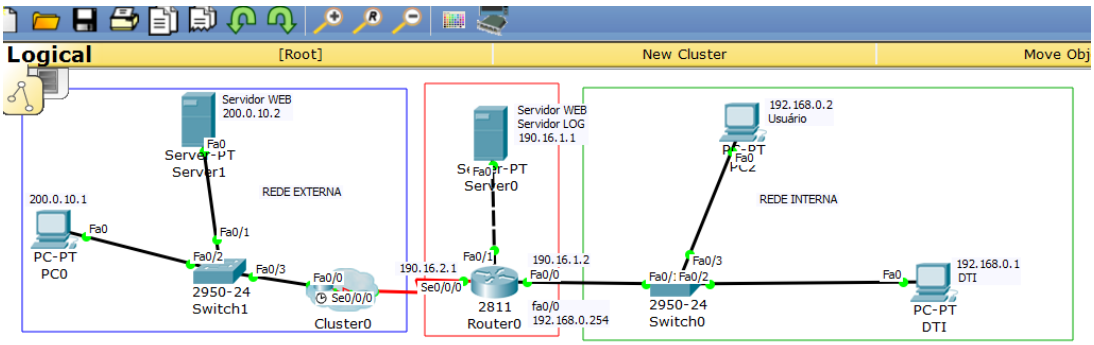
Clique aqui

Produção: inserir como link a figura “Servidor de log no PT_Config_SysLog _NTP1.pkt” anexa ao módulo.

18

3 – Exercício

Nas atividades deste cenário, serão configurados os serviços essenciais de gerenciamento de hosts em uma rede, como serviço de logs centralizado, serviço de sincronização de relógio e monitoramento dos serviços e recursos dos sistemas.



Servidor de log no Packet Tracer

Fonte: O Autor, 2015

Neste exercício, o aluno vai configurar um repositório de Syslog em um servidor da DMZ e enviará os logs dos demais servidores para esse servidor.

O objetivo desta atividade é fazer o aluno aplicar os conceitos de repositório de logs de uma rede e preparar o ambiente para os serviços seguintes, que serão configurados durante o curso, para tanto use o “script” abaixo.

Parte 1: configurar o serviço syslog

etapa 1: ative o serviço syslog, no servidor LOG.

etapa 2: configure os dispositivos intermediários para usarem o serviço syslog.

a. configure Router0 2811para enviar eventos de log ao servidor SV_SYSLOG.

b. configure SW_0 e SW_1 para enviar eventos de log ao servidor SV_SYSLOG.

Parte 2: gerar eventos registrados

etapa 1: altere o status das interfaces para criar logs de eventos.

a. configure uma interface de loopback 0 no Router do Cluster 0 e, em seguida, desative-a.

b. desconecte os PC0 e PC2. em seguida, ative-os novamente.

etapa 2: examine os eventos de syslog.

a. consulte os eventos de syslog.

b. cancele o log antes de passar para a próxima fase.

Parte 3: ajustar manualmente relógios dos switches

etapa 1: ajuste manualmente os relógios nos switches SW_0 e SW_1 à data atual e à hora aproximada.

etapa 2: ative o serviço de logging de data e hora nos switches.

configure SW_0 e SW_1 para enviar seu timestamp com logs que ele envia ao servidor LOG.

Parte 4: configurar o serviço ntp

etapa 1: habilite o serviço ntp. Neste exercício, supomos que o serviço ntp esteja hospedado em um servidor de Internet público (Servidor WB 200.0.10.2).

etapa 2: ajuste automaticamente o relógio automático no roteador Router0-2811 para a data e hora de acordo com o servidor ntp.

etapa 3: ative o serviço de logging de data e hora do roteador.

configure Router0-2811 para enviar seu timestamp com logs que ele envia ao servidor LOG.

Parte 5: verificar os logs de data e hora

etapa 1: altere o status das interfaces para criar logs de eventos.

a. ative novamente e, em seguida, desative a interface de loopback 0 no Router do Cluster0.

b. desconecte os laptops L_1 e L_2. em seguida, ative-os novamente.

etapa 2: examine os eventos de syslog. Consulte os eventos de syslog.

Faça um relatório do que observou.

Clique aqui

Produção: inserir como link a figura “Servidor de log no PT_Config_SysLog _NTP2.pkt” anexa ao módulo.

19

RESUMO

As ferramentas de monitoramento são um subconjunto do universo de ferramentas de gerenciamento focadas na obtenção de informações sobre elementos de infraestrutura de TI.

O Nagios é uma ferramenta de gerenciamento que monitora os elementos e serviços de rede. Ele permite que você faça um gerenciamento da infraestrutura de TI de sua instituição. Os dados são coletados através de testes que simulam o funcionamento de aplicações. O grande destaque dessa ferramenta é a possibilidade de classificação de grupos de usuários para receber relatórios e alertas do sistema.

O Zabbix é uma ferramenta de gerenciamento que monitora os elementos e serviços de rede. Os dados são coletados através de consultas ao SNMP (Simple Network Management Protocol), de ferramentas de testes que simulam o funcionamento das aplicações FTP (File Transfer Protocol), SSH (Secure Shell), HTTP (Hypertext Transfer Protocol) ou através de plugins adicionais que podem ser desenvolvidos e integrados ao Zabbix.

O Cacti é uma ferramenta de monitoração que surgiu como uma opção de frontend (interface gráfica com o usuário para interagir com programas) que apresenta os gráficos dos dados obtidos através de consultas SNMP ou de scripts. O Cacti disponibiliza um ambiente de configuração e operação agradável e acessível (interface web escrita em PHP), com controle de acesso por nível de usuário. O Cacti é muito

usado em monitoramento de links WAN, por conta da sua facilidade na criação de gráficos para monitorar a banda nos links contratados por operadoras.

O Network Traffic Probe (Ntop) é uma ferramenta livre para análise de tráfego de rede. Possui um servidor HTTP (Hypertext Transfer Protocol) e HTTPS (Hypertext Transfer Protocol Secure) nativo, que apresenta uma série de gráficos do tráfego e estatísticas da rede.

As ferramentas apresentadas podem ser classificadas em três grupos:

a) de monitoração de serviços, como Nagios e Zabbix;

b) especializadas na geração de gráficos, como Cacti e Zabbix;

c) de classificação de tráfego, como Ntop.

Quase todas as ferramentas mencionadas são fáceis de instalar. A configuração do Nagios é a mais complexa por exigir a manipulação de vários arquivos de texto. As demais ferramentas possuem interface web para configuração, estando bem documentadas e com vários artigos de referência publicados na internet.

Vimos, também, três exercícios feitos no Packet Tracer, acerca de um servidor de logs, ntp e Syslog.

UNIDADE 2 – SERVIÇOS BÁSICOS DE SEGURANÇA I
MÓDULO 3 – DETECÇÃO E PREVENÇÃO DE INTRUSOS
01

1 - SISTEMAS DE DETECÇÃO DE INTRUSOS (IDS)

Vimos anteriormente como estabelecer um perímetro para proteger uma rede interna dos perigos da internet e de outras redes públicas, incluindo a criação de uma DMZ para prover serviços públicos.

Apesar de ser uma técnica bastante eficiente, existe a possibilidade de nossas defesas serem atacadas e vencidas. Lembre-se: não existe sistema 100% seguro e isso sempre vai existir. Para minimizar esse problema existe a **detecção e a prevenção de intrusos**, que consiste no monitoramento constante de diversos elementos, como segmentos de rede, sistemas operacionais e aplicações.

Através desse monitoramento constante, podemos tomar uma ação caso alguma atividade suspeita seja detectada, que pode ser desde um alerta para o administrador de segurança até o bloqueio temporário ou permanente do atacante.

Considera-se um IDS (Intrusion Detection System), em conjunto com um *firewall*, como uma **aplicação do princípio de defesa em profundidade**. Uma ferramenta IDS serve basicamente para nos trazer informações sobre nossa rede, tais como:

- Quantas tentativas de ataques a rede sofre por dia;

- Qual tipo de ataque foi usado;
- Qual a origem dos ataques.

E você, o que entende por detecção e prevenção de intrusos?

Veja aqui uma possível resposta.

Veja aqui

Detecção de intrusos é a identificação de uma requisição ou atividade maliciosa que pode causar danos na rede de computadores e prevenção é bloquear a atividade maliciosa para impedir que a mesma cause dano na rede de computadores.

02

Sistema de detecção de intrusos ou Sistema de detecção de intrusão (**Intrusion detection system - IDS**) refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um cracker ou até mesmo de funcionários mal intencionados (atividade maliciosa).

De modo simples, um IDS é uma ferramenta capaz de detectar atividade maliciosa através do monitoramento constante de um segmento de rede ou de chamadas de sistema em um sistema operacional.

Existem diversos IDS no mercado com componentes e funcionamento distintos, porém normalmente encontramos os seguintes componentes em um IDS:

Sensor

Responsável por coletar informações sobre a rede, sistema operacional ou aplicação, para ser utilizado como parâmetro de entrada para o sistema de detecção.

Engine

Responsável por analisar as informações coletadas e comparar com um padrão conhecido, para assim, determinar se é um evento normal ou malicioso. Algumas engines trabalham com elementos mais determinísticos, como assinaturas de ataque. Outras trabalham com redes neurais e sistemas estatísticos, e podem detectar ataques desconhecidos.

Console

Interface para o administrador configurar o funcionamento da ferramenta.

Esses componentes podem estar em uma única máquina (**centralizados**) ou **distribuídos**.

Existem ainda diferentes tipos de IDS de acordo com o modo de funcionamento, local e forma de atuação frente a um ataque que serão vistos a seguir.

03

2 – Classificações dos IDS

Os IDS podem ser classificados conforme ao modo de funcionamento, ao local de atuação e à forma de atuação, conforme veremos a seguir.

Quanto ao **modo de funcionamento**, podem ser:

Detector de anomalias

Utiliza alguma função estatística ou rede neural para definir um perfil de utilização normal da rede em uma etapa de aprendizado. Em seguida, analisa constantemente o padrão atual com o aprendido. Caso ocorra algum desvio acima de um limiar, considera que houve uma tentativa de intrusão. Essa técnica tem a vantagem de possibilitar a detecção de ataques desconhecidos, mas pode gerar falsos positivos e não é capaz de saber o ataque específico em ação.

Detector de mau uso

É o modo mais utilizado atualmente. Possui funcionamento parecido com o de um antivírus. Através de um conjunto de assinaturas previamente configuradas, o IDS monitora o ambiente em busca de eventos que coincidam com alguma assinatura. Possui baixo índice de falsos positivos caso as assinaturas sejam de boa qualidade. Não detectam ataques desconhecidos e dependem de atualização das assinaturas por parte do fabricante ou da comunidade.

04

Quanto ao **local de atuação**, podem ser:

Baseados em host (HIDS)

Agem em cima de uma única máquina. Normalmente são instalados na própria máquina que se deseja proteger e monitoram chamadas do sistema operacional ou atividades de uma aplicação específica. Comumente chamados de Host-based IDS (HIDS).

Baseados em redes (NIDS)

Agem em cima de um segmento de rede. São instalados em uma máquina que faz parte do segmento de rede. Monitoram o tráfego no segmento de rede do qual a interface de monitoramento faz parte. Os IDSs de rede são chamados de NIDS. Um NIDS é capaz de detectar atividade suspeita em uma rede inteira que se encontra atrás dele, porém, como age no nível do sistema operacional, um HIDS é capaz de obter informações mesmo que elas não trafeguem pela rede. Em arquiteturas reais, é muito comum a combinação de NIDS e HIDS de modo a obter uma proteção mais completa.

05

Quanto à **forma de atuação**, podem ser:

Reativos	Passivos	Ativos
Agem após um evento malicioso. Podem inserir regras em um firewall acoplado ou tentar encerrar a conexão utilizando pacotes falsificados. É importante ressaltar que, em alguns ataques, a reação pode ser tardia demais. Existem ataques em que um pacote é suficiente para causar algum tipo de estrago. Nesses casos, no momento em que o IDS reagir ao ataque, será tarde demais.	Não causam nenhuma alteração no ambiente. Fazem apenas registros dos eventos e notificações para os administradores. Uma vantagem de um IDS passivo é que ele não causa nenhuma interrupção na rede caso falhe, porém o tráfego malicioso deixará de ser detectado. Aqui temos uma aplicação inversa do princípio de fail safe.	Agem ativamente em caso de evento malicioso. Os sistemas ativos são chamados de Sistemas de Prevenção de Intrusos ou IPS.

06

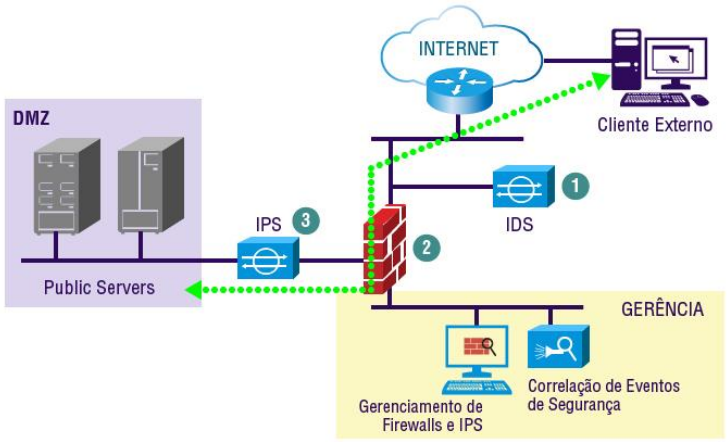
3 - Sistema de Prevenção de Intrusos (IPS)

O **IPS** (Intrusion Prevention System) se diferencia do IDS pelo fato de ser **ativo**, ou seja, interfere diretamente nos eventos que passam por ele. Diferentemente o IDS, que é passivo, apenas monitora os eventos sem neles interferir.

O IPS é complemento do IDS, pois bloqueia a intrusão. Ele detecta e bloqueia a invasão.

Os IPSs mais comuns são os de **rede**, que atuam em cima do tráfego de rede.

Na figura abaixo, podemos diferenciar um IDS de um IPS, por meio da sua localização na rede.



Posicionamento do IDS e do IPS
Fonte: Internet, 2015.

Na imagem podemos perceber que o tráfego passa diretamente pelo IPS (3), de modo que o sistema pode optar por não transmitir um tráfego adiante, caso suspeite que seja malicioso. Esse comportamento é diferente do comportamento do IDS (1), que apenas monitora o tráfego. Mesmo que o IDS tome uma ação, essa será reativa, pois não vai interferir no tráfego da rede. Veja que o firewall (2) encontra-se entre o IDS e o IPS.

07

Uma **vantagem** dos IPSs é a possibilidade de bloquear um ataque a partir do seu primeiro pacote, o que pode ser fundamental para mitigá-lo, visto que em alguns ataques, basta um pacote para que o ataque seja bem-sucedido (lembre-se do ping da morte).

Uma **desvantagem** do IPS é a sua necessidade de capacidade de processamento suficiente para analisar todos os pacotes que passam por ele, o que pode causar atrasos em casos de redes muito sobrecarregadas; isso não ocorre no IDS, que é passivo. Um IDS sobrecarregado, porém, não consegue analisar todos os pacotes que passam por ele, de modo a se tornar um IDS estatístico, pois analisa apenas uma porcentagem do tráfego.

Em muitos IPSs comerciais, o fabricante indica a taxa de transferência máxima (*troughput*) que um determinado IPS é capaz de suportar.

Outra característica importante a ser considerada em um IPS é a **ação em caso de falha**. Um IPS onde ocorreu uma falha pode bloquear ou liberar todas as conexões que passam por ele. Essa decisão é capciosa e complexa, pois liberar todas as conexões pode permitir que um atacante acesse a rede protegida, e bloqueá-las pode causar um problema de disponibilidade.

Então, como podemos **diferenciar um IPS de um IDS**?

Veja a resposta.

Veja a resposta

O IDS somente detecta a intrusão, porém não bloqueia a mesma. O IPS detecta e bloqueia a invasão. O IDS é reativo e o IPS é ativo.

08

4 – HIDS E NIDS

O HIDS (Host Intrusion Detection Systems) ou Sistema Hospedeiro de Detecção de Intrusos é um sistema computadorizado de segurança de rede utilizado para proteção contra vírus, *spyware*, *malware* e outros tipos maliciosos de arquivo. São instalados em certos pontos de interseção, como servidores e roteadores.

HIDS agem em uma máquina específica realizando:

a) Monitoramento;

b) System calls;

c) Logs de aplicação;

d) Modificação em arquivos;

e) Criação de processos.

Exemplos de programas HIDS:

a) OSSEC;

b) SAMHAIN;

c) Tripwire;

d) Osíris.

Na maior parte dos casos, quando se fala em IDS, refere-se **aos sistemas de detecção de intrusos baseados em rede** (NIDS), que são mais comuns.

Um **NIDS - sistema baseado em rede** é capaz de monitorar um segmento de rede e detectar tráfego malicioso destinado a qualquer máquina que se encontre atrás do segmento monitorado, criando uma proteção mais abrangente, porém limitada a informações obtidas através de pacotes enviados na rede.

09

Como complemento aos NIDSs, existem sistemas de detecção que agem em uma máquina específica, monitorando elementos como chamadas ao sistema (system calls), logs de aplicação, modificação em arquivos ou registros, criação de processos, entre outros, por exemplo, os HIDS (Host Intrusion Detection Systems).

Fique Atento!

Os HIDS protegem apenas a máquina onde estejam instalados, porém são capazes de obter informações que não trafegam na rede.

Existem diversos **tipos** de HIDSs. Os mais simples monitoram questões simples de um ambiente computacional, como alterações em arquivos, uso excessivo de CPU, memória etc. Outros, mais complexos, se instalam como drivers ou módulos do kernel, monitorando elementos de baixo nível no sistema operacional, como chamadas ao sistema e acesso físico ao disco, entre outros.

É comum a combinação de NIDS e HIDS em uma rede, de modo a monitorar tanto a rede, quanto as aplicações e sistemas operacionais.

As tecnologias de IDS atualmente estão bastante sedimentadas, de modo que existem diversas ferramentas, livres e comerciais. Nesta disciplina recomendaremos o **Snort**, considerado um dos melhores IDS open source do mercado.

10

5 - SNORT

O SNORT é uma ferramenta NIDS, open-source, desenvolvida por Martin Roesch. Tornou-se popular por sua flexibilidade nas configurações de regras e constante atualização frente às novas ferramentas de invasão. Tem estrutura modular altamente customizável com plugins, disponível em diversas plataformas (arquitetura modular).

Outro ponto forte desta ferramenta é o fato de ter o maior cadastro de assinaturas, ser leve, pequeno, fazer escaneamento do micro e verificar anomalias dentro de toda a rede ao qual seu computador pertence.

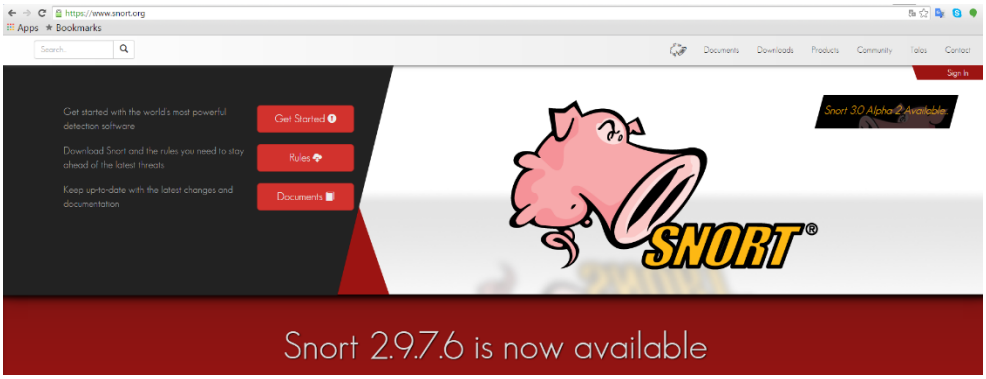


Figura 18: Site do Snort
Fonte: www.snort.org, 2015.

Como o SNORT é baseado em assinaturas com plugin estatístico (SPADE), é necessário que ele seja constantemente atualizado para continuar eficaz.

11

Por ter o código-fonte aberto, o Snort foi portado para plataformas como Linux e Windows. A figura a seguir apresenta os diferentes componentes do Snort, desde a captura do pacote na rede até o registro de um alerta ou log.

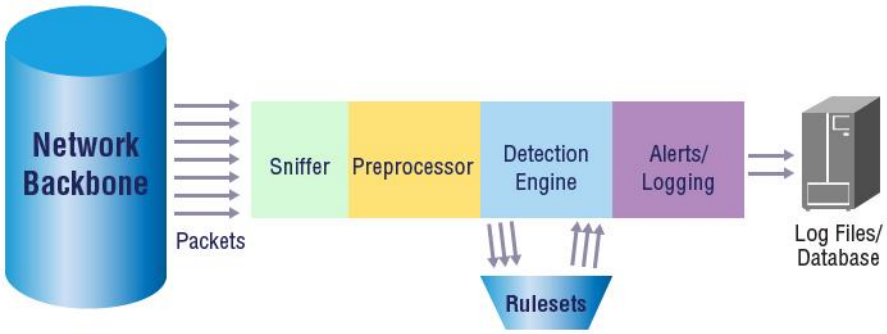


Figura 19: Componentes do Snort.
Fonte: Internet, 2015.

Na figura acima o Network Backbone é a nossa Internet de onde chegam os pacotes (Packets) que passam por um decodificador de pacote simbolizado pelo Sniffer. O decodificador de pacote é responsável pela obtenção dos pacotes no segmento de rede monitorado. Os preprocessadores (Preprocessor) realizam diversos tipos de processamento em cima dos pacotes, com o objetivo de obter tráfego normalizado. Questões como fragmentação, uso de codificações diferentes e ofuscação de pacotes são tratadas nessa etapa.

Em seguida, o Detection Engine é responsável por compilar as regras (assinaturas) e testar os pacotes contra essas regras. O registro e sistema de alerta gera os registros do Snort e envia os alertas. Por fim, os módulos de saída exportam os alertas e registros para um arquivo ou banco de dados (Log Files/Database).

12

O Snort possui uma estrutura modular altamente personalizável, onde diversos plugins e programas acessórios podem ser usados para expandir suas funcionalidades, tais como a possibilidade de reagir a um alerta, a atualização automática das suas assinaturas e o gerenciamento de diversos sensores espalhados em uma ou mais redes.

Fique Atento!

Através da arquitetura modular do Snort, é possível a geração de alertas em arquivos texto, bases de dados, entre outros. Em conjunto com os alertas, é possível ainda o armazenamento dos pacotes que causaram um determinado alerta, o que é importante para se determinar se um alerta é legítimo, ou se é um falso-positivo.

Há programas auxiliares ao Snort, que geram alertas em formatos mais úteis para um administrador, tais como:

- BASE (Basic Analysis and Security Engine),
- Sguil (The Analyst Console for Network Security Monitoring) e
- OSSIM, considerado um SIEM (Security Information and Event Management).

O OSSIM é um conjunto de ferramentas integradas, com um console gráfico completo. Muitas das ferramentas presentes no OSSIM foram ou serão apresentadas neste curso, como Snort, Nessus, Ntop e Nagios. O interessante do OSSIM é que ele é disponibilizado como uma imagem ISO, com todos os componentes instalados automaticamente, bastando apenas a sua inicialização através dessa ISO.

SIEM

Um SIEM é uma ferramenta centralizada de segurança, com o objetivo de concentrar as informações de segurança em uma única ferramenta.

13

Abaixo temos um **exemplo de alerta** gerado pelo Snort. A explicação de cada linha segue abaixo.

[**][1:2001669:2] BLENDING-EDGE Web Proxy Get Request[**] [Classification: Potentially Bad Traffic][Priority 2]

09/22-04:09:54.54.944632 192.168.1.1:64570-> 192.168.2.33:80

TCP TTL:108 TOS:0x0 ID:17008 IpLen: 20 DgmLen: 454 DF

APSeq: 0x478a75AC Ack: 0x4F338167 Win: 0x40B0 TcpLen: 20

[Xref=>http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0951] [Xref=>http://www.secutiryfocus.com/bid/1756] [Xref=>http://www.whitehats.com/info/IDS474]

Onde:

a) **2001669** = Gerador da regra (GID);

b) **2** = Código da regra (SID);

c) **BLENDING-EDGE** = Revisão;

d) **Web Proxy Get Request[**] [Classification: Potentially Bad Traffic][Priority 2]** = Descrição do alerta + classificação + prioridade;

e) **09/22-04:09:54.54.944632 192.168.1.1:64570-> 192.168.2.33:80** = Timestamp + IP + portas;

f) ***AP***Seq: 0x478a75AC Ack: 0x4F338167 Win: 0x40B0 TcpLen: 20** = Parâmetros de rede;

g) **[Xref=>http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0951], [Xref=>http://www.secutiryfocus.com/bid/1756], [Xref=>http://www.whitehats.com/info/IDS474]** = Referências.

Na próxima etapa do nosso estudo, veremos como instalar, configurar e extrair as informações necessárias do Snort.

14

RESUMO

Vimos anteriormente como estabelecer um perímetro para proteger uma rede interna dos perigos da internet e de outras redes públicas, incluindo a criação de uma DMZ para prover serviços públicos.

Através desse monitoramento constante, podemos tomar uma ação caso alguma atividade suspeita seja detectada, que pode ser desde um alerta para o administrador de segurança até o bloqueio temporário ou permanente do atacante.

Considera-se um IDS (Intrusion Detection System), em conjunto com um firewall, como uma aplicação do princípio de defesa em profundidade.

Um IDS consiste em uma ferramenta capaz de detectar atividade maliciosa através do monitoramento constante de um segmento de rede ou de chamadas de sistema em um sistema operacional. Possui os seguintes componentes: Sensor, Engine e Console. Esses sistemas podem ser Centralizados ou Distribuídos.

Quanto ao modo de funcionamento eles podem ser de: a) Detector de anomalias e b) Detector de mau uso.

Quanto ao local de atuação: a) Baseados em host (HIDS) e b) Baseados em redes (NIDS)

Quanto à forma de atuação: a) Reativos; b) Passivos e c) Ativos.

O IPS (Intrusion Prevention System) se diferencia do IDS pelo fato de ser ativo, ou seja, interfere diretamente nos eventos que passam por ele. Diferentemente o IDS, que é passivo, apenas monitora os eventos sem neles interferir. Os IPSs mais comuns são os de rede, que atuam em cima do tráfego de rede.

HIDS agem em uma máquina específica realizando: a) Monitoramento; b) System calls; c) Logs de aplicação; d) Modificação em arquivos; e) Criação de processos.

Na maior parte dos casos, quando se fala em IDS, refere-se aos sistemas de detecção de intrusos baseados em rede (NIDS), que são mais comuns. Um sistema baseado em rede é capaz de monitorar um segmento de rede e detectar tráfego malicioso destinado a qualquer máquina que se encontre atrás do segmento monitorado, criando uma proteção mais abrangente, porém limitada a informações obtidas através de pacotes enviados na rede.

Como complemento aos NIDSs, existem sistemas de detecção que agem em uma máquina específica, monitorando elementos como chamadas ao sistema (system calls), logs de aplicação, modificação em arquivos ou registros, criação de processos, entre outros, por exemplo, os HIDS.

Esses sistemas são chamados de HIDS (Host Intrusion Detection Systems). Um HIDS protege apenas a máquina onde esteja instalado, porém é capaz de obter informações que não trafegam na rede.

Snort é NIDS open source baseado em assinaturas com plugin estatístico (SPADE). Tem estrutura modular altamente customizável com plugins, disponível em diversas plataformas (arquitetura modular).

Através da arquitetura modular do Snort, é possível a geração de alertas em arquivos texto, bases de dados, entre outros. Em conjunto com os alertas, é possível ainda o armazenamento dos pacotes que causaram um determinado alerta, o que é importante para se determinar se um determinado alerta é legítimo, ou se é um falso-positivo.

UNIDADE 2 – SERVIÇOS BÁSICOS DE SEGURANÇA I
MÓDULO 4 – SNORT
01

1 – OBTENÇÃO DO SNORT PARA O LINUX

No caso do Linux, a própria distribuição Debian, recomendada para que cada um instale na máquina própria, provê o Snort já compilado, de modo que basta uma conexão com a internet e dois comandos para instalar a parte básica do Snort:

```
apt-get update

apt-get install snort
```

O primeiro comando atualiza a base de pacotes do Debian e o segundo comando efetivamente instala a última versão do Snort disponível. É importante ressaltar que o Debian nem sempre disponibiliza as últimas versões dos programas, pois os desenvolvedores possuem um rígido processo de inclusão de

novas versões, de modo que a versão disponibilizada normalmente é inferior à última versão disponível no site.

Caso o aluno necessite de uma versão mais atualizada, recomenda-se utilizar o conjunto de pacotes *unstable* ou utilize outra distribuição com atualizações mais frequentes, como o Ubuntu (por questão de conhecimento a que recomendo).

Caso tudo corra bem, teremos o seguinte resultado: clique aqui

Algumas das instruções podem aparecer diferentes das obtidas aqui.

Clique aqui

Jksobue:~# apt-get install snort

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following extra packages will be installed:

libcompress-raw-zlib-perl libcompress-zlib-perl libfont-afm-per

libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl

libhtml-tree-perl libio-compress-base-perl libio-compress-zlib-perl libltdl3

libmailtools-perl libmysqlclient15off libpcap0.8 libprelude2

libtimedate-perl liburi-perl libwww-perl mysql-common oinkmaster

snort-common snort-common-libraries snort-rules-default

Suggested packages:

libio-socket-ssl-perl snort-doc

The following NEW packages will be installed:

libcompress-raw-zlib-perl libcompress-zlib-perl libfont-afm-perl

libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl

libhtml-tree-perl libio-compress-base-perl libio-compress-zlib-perl libltdl3

libmailtools-perl libmysqlclient15off libpcap0.8 libprelude2

```
libtimedate-perl liburi-perl libwww-perl mysql-common oinkmaster snort

snort-common snort-common-libraries snort-rules-default

0 upgraded, 23 newly installed, 0 to remove and 0 not upgraded.

Need to get 5314kB of archives.

After this operation, 18.3MB of additional disk space will be used.

Do you want to continue [Y/n]? Y

[...]

Fetched 5314kB in 7s (737kB/s)

Preconfiguring packages ...

Selecting previously deselected package mysql-common.

(Reading database ... 19042 files and directories currently installed.)

[...]

Processing triggers for man-db ...

Setting up mysql-common (5.0.51a-24+lenny4) ...

Setting up libmysqlclient15off (5.0.51a-24+lenny4) ...

Setting up libpcap0.8 (0.9.8-5) ...

Setting up libltdl3 (1.5.26-4+lenny1) ...

Setting up libprelude2 (0.9.18.1-1) ...

Setting up snort-common-libraries (2.7.0-20.4) ...

Setting up snort-rules-default (2.7.0-20.4) ...

Setting up snort-common (2.7.0-20.4) ...

Setting up snort (2.7.0-20.4) ...

Stopping Network Intrusion Detection System : snortNo running snort instance found (warning).

Starting Network Intrusion Detection System : snort (eth0 no /etc/

snort/snort.eth0.conf found, defaulting to snort.conf ...done).
```

```
Setting up libcompress-raw-zlib-perl (2.012-1lenny1) ...

Setting up libio-compress-base-perl (2.012-1) ...

Setting up libio-compress-zlib-perl (2.012-1) ...

Setting up libcompress-zlib-perl (2.012-1) ...

Setting up libfont-afm-perl (1.20-1) ...

Setting up libhtml-tagset-perl (3.20-2) ...

Setting up liburi-perl (1.35.dfsg.1-1) ...

Setting up libhtml-parser-perl (3.56-1+lenny1) ...

Setting up libhtml-tree-perl (3.23-1) ...

Setting up libhtml-format-perl (2.04-2) ...

Setting up libtimedate-perl (1.1600-9) ...

Setting up libmailtools-perl (2.03-1) ...

Setting up libwww-perl (5.813-1) ...

Setting up oinkmaster (2.0-2) ...

Jksobue:~#
```

02

Algumas partes do resultado da instalação (representadas pelas linhas contendo [...]) foram suprimidas por questão de tamanho. Ao final da execução do comando, o Snort estará instalado e executando. Durante a instalação será perguntado o endereço da rede local, que corresponderá ao parâmetro HOME_NET. Esse parâmetro é importante, pois o tráfego que não se originar ou tiver como destino essa rede será ignorado pelo Snort.

Caso queira monitorar todo o tráfego que passa pela interface de captura do IDS, configure HOME_NET como 0.0.0.0/0.

Com o Snort instalado, podemos verificar se está em execução utilizando o **comando ps no Linux**:

```
Jksobue:/var/log/snort# ps aux | grep snort
```

```
snort    3305 26.6 58.1 174664 149108 ?      S<s  03:54   5:11 / usr/sbin/snort -m 027 -D -d -l
/var/log/snort -u snort -g snort -c / etc/snort/snort.conf -S HOME_NET=[172.16.1.0/24] -i eth0
```

Verifique que uma série de parâmetros é repassada para o Snort automaticamente, por conta da instalação do Snort no Debian (Ubuntu). Os principais serão descritos a seguir.

Caso tenha interesse em outros parâmetros do Snort, o comando **man snort** apresenta uma descrição de todos os parâmetros existentes.

Alguns desses parâmetros podem ser ajustados no arquivo /etc/default/snort. Para controlar a execução do serviço do Snort, podemos utilizar os seguintes comandos:

a) **/etc/init.d/snort stop** – encerra o Snort.

b) **/etc/init.d/snort start** – inicia o Snort.

c) **/etc/init.d/snort restart** – reinicia o Snort (aplica mudanças no arquivo de configuração).

Parâmetros

a) **-D**: modo daemon, executa o Snort como um serviço, de modo que ele ficará em constante execução até que seu processo seja finalizado.

b) **-d**: instrui o Snort a incluir os dados da camada de aplicação no pacote que será registrado.

c) **-l**: indica o diretório onde os logs do Snort serão armazenados. No acaso, o diretório /var/log/snort conterá os registros de alertas e pacotes.

d) **-u**: indica o usuário que será utilizado para executar o Snort. Conforme o princípio do menor privilégio, não se recomenda que o Snort seja executado com direitos de administrador (root).

e) **-g**: indica o grupo utilizado para executar o processo do Snort.

f) **-c**: indica o caminho do arquivo de configuração.

g) **-S**: variável=valor ajusta a variável para o valor definido. Permite alteração em linha de comando de parâmetros do arquivo de configuração. Na execução acima, o parâmetro está ajustando a variável HOME_NET para o valor 172.16.1.0/24, definido durante a instalação.

h) **-i**: indica a interface que será utilizada para a captura de tráfego.

2 - CONFIGURAÇÃO DO SNORT

A configuração do Snort reside no arquivo /etc/snort/snort.conf. Esse arquivo é extenso e contém uma série de parâmetros de configuração do Snort.

Para efeito da disciplina, serão vistos alguns parâmetros mais importantes. O aluno que desejar se aprofundar mais a respeito dos parâmetros de configuração do Snort pode buscar mais informações no manual da ferramenta.

a) Variáveis (var) – configuram parâmetros do Snort, como a rede local, a rede externa, os servidores DNS, SMTP, HTTP, SQL, Telnet e SNMP (Simple Mail Transfer Protocol é o protocolo de envio de mensagens de correio eletrônico).

Configurar esses parâmetros pode reduzir significantemente a quantidade de falsos positivos no seu IDS, pois o Snort só alertará quando o destino efetivamente dispor do serviço indicado. Veja aqui alguns exemplos.

b) var RULE_PATH – indica o caminho onde os arquivos de regras (assinaturas) se encontram.

c) include $RULE_PATH/<arquivo>.rules – inclui um arquivo de regras. Os arquivos de regras normalmente são divididos por categorias, de modo que seja fácil comentar as linhas correspondentes para desabilitar as regras. Os comentários são feitos utilizando o caractere “#” no início da linha.

Veja aqui

A seguir alguns exemplos.

a) var HOME_NET [192.168.1.0/24]

b) var SMTP_SERVERS 172.16.1.20

c) var EXTERNAL_NET any

3 - REGRAS DO SNORT

As regras do Snort são elementos-chave para a configuração do mesmo. Sem essas regras, o Snort torna-se um mero analisador de pacotes. As regras são linhas de texto contendo instruções para o Snort localizar pacotes que contenham características específicas e informações acerca do alerta a ser gerado.

Abaixo um exemplo de regra, que detecta um ataque específico para servidores de correio eletrônico (SMTP).

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"SMTP RCPT TO overflow";
flow:to_server,established; content:"rcpt to|3A|"; nocase; isdataat:300,relative; pcre:"/^RCPT
TO\x3a\s[^\n] {300}/ism"; reference:bugtraq,2283; reference:bugtraq,9696; reference:cve,2001-
0260; classtype:attempted-admin; sid:654; rev:14;)
```

Observe as variáveis do arquivo *snort.conf*, as portas envolvidas (25 TCP) e a indicação da mensagem de alerta (parâmetro msg).

As regras instaladas no Snort podem ser habilitadas ou desabilitadas, individualmente ou em grupo, inserindo comentários (#) nos arquivos de regra (extensão .rules) ou no próprio snort.conf, para bloquear um conjunto inteiro de regras.

Muitas regras podem gerar muitos **falsos positivos**, então fazer um ajuste das regras é uma tarefa cansativa, porém indispensável para que os registros de alerta sejam confiáveis e úteis. Um IDS que gera muitos alertas falsos facilmente acaba em desuso. Existem atualmente diferentes conjuntos de regras para o Snort, alguns pagos e outros gratuitos.

05

A seguir uma descrição sobre os conjuntos mais comuns:

a) Regras Sourcefire VRT (Vulnerability Research Team) Certified

Regras fornecidas pela Sourcefire, empresa responsável pelo desenvolvimento do Snort. Necessitam de uma assinatura por parte do usuário.

b) Regras Sourcefire VRT Certified (versão para usuários registrados)

Regras gratuitas (snort-rules), fornecidas com defasagem de 30 dias em relação às regras comerciais, podem ser obtidas mediante registro no sítio. As regras se referem a versões específicas do Snort, portanto verifique a versão instalada antes de baixá-las.

c) Regras Emerging Threats

Regras comunitárias e gratuitas, desenvolvidas por voluntários. Apesar de gratuitas, as regras ET (Emerging Threats) são muito eficientes e possuem um elevado índice de atualizações. O diretório open contém as regras para cada versão do Snort.

d) Regras Emerging Threats Pro

Versão paga do ET, que custava 500 dólares por ano. Para instalar um novo conjunto de regras, basta copiar os arquivos para o diretório de regras do Snort (normalmente /etc/snort/rules) e referenciá-los no arquivo snort.conf (include <caminho do arquivo .rule>).

06

4 - OINKMASTER

Conforme dito no item anterior, a atualização constante de regras é fundamental para o bom funcionamento de um IDS. Porém, dependendo do número de atualizações diárias e da quantidade de sensores, a tarefa de mantê-los atualizados pode ficar muito complexa.

Com o intuito de facilitar a atualização de regras, foi criada uma ferramenta chamada Oinkmaster, que permite que a atualização seja feita de forma automática.

A instalação do Oinkmaster é automaticamente realizada junto com o Snort, durante a execução do comando apt-get install.

A configuração da ferramenta é bastante simples e consiste apenas em indicar no arquivo de configuração os parâmetros necessários e instalar um agendamento cron (sistema de agendamento de tarefas de um ambiente Unix) no ambiente para executar periodicamente a ferramenta.

Mais informações sobre o funcionamento do Oinkmaster podem ser obtidas no documento Installing and configuring OinkMaster, de Patrick Harper.

07

A seguir, os passos para a configuração do Oinkmaster para atualização das regras do projeto emerging threats.

1. Edite o arquivo /etc/oinkmaster.conf e adicione a seguinte linha:

http://www.emergingthreats.net/rules/emerging.rules.tar.gz

Salve o arquivo.

2. Verifique o funcionamento do Oinkmaster, executando-o na linha de comando:

/usr/sbin/oinkmaster –C /etc/oinkmaster.conf –o <diretório de saída>

3. Crie um novo diretório para não misturar os conjuntos de regras (ex: /etc/snort/rules2).

4. Configure o cron para executar o Oinkmaster periodicamente com o comando crontab –e. Exemplo para executar o Oinkmaster todos os dias às 5h30 da manhã:

30 5 * * * /usr/sbin/oinkmaster –C /etc/oinkmaster.conf –o /etc/ snort/rules2

5. É necessário reiniciar o Snort após a atualização, então é interessante criar um script para realizar as duas tarefas e inclui-lo no cron.

6. Adicione os arquivos de regras no seu snort.conf, utilizando as diretivas include <arquivo.rule>. Não se esqueça de especificar o caminho completo.

O Oinkmaster possui parâmetros extras que podem ser inseridos no arquivo de configuração.

Parâmetros extras

Seguem dois parâmetros importantes:

a) **enablesid SID1, SID2, ...** – habilita automaticamente a regra identificada pelo SID. Um SID é um número único que identifica uma regra, que pode ser visto no parâmetro “sid:” presente na linha da regra.

b) **disablesid SID1, SID2, ...** – desabilita automaticamente a regra identificada pelo SID.

08

5 - GUARDIAN: UM SNORT REATIVO

O Guardian é um script na linguagem Perl, que insere temporariamente regras de bloqueio em um firewall, a partir dos alertas gerados pelo Snort. Através do Guardian, a instalação de Snort passa a ter uma característica reativa.

O Guardian não é instalado automaticamente na distribuição e deve ser baixado e instalado manualmente.

Os passos a seguir instalam o Guardian e o integram com o firewall Iptables:

1) Baixe a última versão do “Guardian Active Response for Snort” e o descompacte.

2) Copie o arquivo de configuração do Guardian para o diretório /etc.

3) Edite o arquivo e ajuste os seguintes parâmetros:

3.1) Interface – interface onde serão bloqueados os pacotes maliciosos. Ajuste para a sua interface externa.

3.2) HostGatewayByte – último octeto do endereço IP do gateway.

3.3) AlertFile – local do arquivo de alertas do Snort.

4) Crie o arquivo /etc/guardian.ignore e inclua nele os endereços IP que serão ignorados (um por linha).

5) Crie o arquivo /etc/guardian.target e inclua nele os endereços IP da máquina atual.

6) Copie o arquivo guardian.pl para o diretório /usr/local/bin.

7) Copie os scripts de bloqueio e desbloqueio referentes ao Iptables para o mesmo diretório.

7.1) cp scripts/iptables_unblock.sh /usr/local/bin/guardian_unblock.sh

7.2) cp scripts/iptables_block.sh /usr/local/bin/guardian_block.sh

8) Execute o Guardian com o seguinte comando:

/usr/local/bin/guardian.pl –c /etc/guardian.conf

09

6 - SNORT-INLINE

O Snort-inline é um modo especial de funcionamento do Snort, integrado com o firewall Iptables/ netfilter para funcionar como um IPS.

Funcionamento:

a) Pacotes recebidos pelo Iptables são encaminhados para uma fila.

b) Snort-inline decide pelo encaminhamento.

Cada pacote recebido pelo Iptables é encaminhado para uma fila (queue), para ser processado pelo Snort-inline, que pode descartar pacotes de acordo com as suas regras, de modo que o pacote não é passado adiante pelo processo de roteamento do firewall. Opcionalmente podem ser gerados registros e alertas correspondentes.

Assim como qualquer IPS, a implementação do Snort-inline deve ser realizada com cuidado, pois caso a máquina onde se encontra o IPS fique sobrecarregada, ela pode impactar negativamente no desempenho da rede ou até tornar indisponível o segmento de rede atrás do IPS.

Um dos principais usos do Snort-inline consiste no Projeto Honeynet (**Honeynet Project**). Ele foi utilizado como componente principal do honeywall roo (*firewall* da rede de potes de mel).

Dessa forma, um pesquisador de segurança consegue aprender com as técnicas empregadas pelo atacante. Uma honeynet é um tópico avançado e deve ser utilizada apenas por administradores experientes. Saiba+

Os responsáveis pelo projeto Snort-inline passaram a investir em um novo IDS/IPS open source, chamado **suricata**. Apesar de recente, ele possui objetivos ambiciosos, podendo vir a ser um novo padrão em IDS/IPS open source. As regras Emerging Treats também estão disponíveis para o Suricata da Open Information Security Foundation (OISF).

Honeynet

Uma honeynet consiste em uma rede com servidores especialmente construídos com o objetivo de atrair atacantes para a honeynet (daí o honey, “mel” em inglês) ou “rede de potes de mel”).

Saiba+

Mais informações sobre o projeto Honeynet podem ser encontradas em: http://www.honeynet.org/.

10

6.1 - Bro Intrusion Detection System

Outro projeto de IDS é o HLBR, desenvolvido no Brasil e disponível no sourceforge.

O Bro IDS é um projeto open source de um sistema de detecção de intrusos baseado em rede. Forte concorrente do Snort, ele monitora de forma passiva o tráfego de rede em busca de atividades suspeitas.

A sua análise inclui a detecção de ataques específicos (inclusive os definidos pelas assinaturas, mas também aqueles definidos em termos de eventos) e atividades incomuns (por exemplo, certo host conectar a determinados serviços ou falhas em tentativas de conexão).

Se o Bro detectar algo de interesse, pode ser configurado para gerar uma entrada de log, alertar o operador em tempo real, executar um comando do sistema operacional (por exemplo, para finalizar a conexão ou bloquear um host malicioso on-the-fly).

Além disso, os arquivos de log detalhados do Bro podem ser facilmente utilizados pela ciência forense.

Para que esse aplicativo funcione corretamente, será necessário instalar os seguintes componentes na máquina Linux: Libpcap, Flex, Bison ou byacc, cabeçalhos e bibliotecas do BIND8, Autotools, OpenSSL, Libmagic, Libz, GnuPG, LibGeopIP e Google Perftools.

HLBR

O HLBR é um projeto brasileiro destinado à segurança em redes de computadores. O HLBR é um IPS (Intrusion Prevention System) bastante eficiente e versátil, podendo ser usado até mesmo como bridge para honeypots e honeynets. Como não usa a pilha TCP/IP do sistema operacional, ele é "invisível" a outras máquinas na rede e atacantes, pois não possui número de IP.

11

7 – HIDS - Host-based Intrusion Detection System

Existem diversas ferramentas que realizam detecção de intrusos com base em hosts.

Podemos citar algumas, disponíveis na internet:

a) OSSEC

b) SAMHAIN

c) Tripwire

d) Osíris

OSSEC
Ferramenta bastante completa de HIDS, capaz de realizar análise de logs, verificação de integridade de arquivos, monitoramento de políticas, detecção de rootkits e alertas em tempo real, entre outros. Disponível para plataformas como Linux, MacOS, Solaris, HP-UX, AIX e Windows.

SAMHAIN
HIDS que provê verificação de integridade de arquivos e análise e monitoramento de arquivos de log. Ele foi projetado para monitorar múltiplas máquinas com diferentes sistemas operacionais, provendo registros centralizados e gerenciados.

Tripwire
Ferramenta antiga de monitoramento de integridade de arquivos, muito usada para verificar se os arquivos de um sistema operacional foram modificados, o que pode ser um indício de comprometimento do servidor.

Osíris
Ferramenta de monitoramento de alterações em máquinas capaz de monitorar mudanças no sistema de arquivos, lista de usuários e grupos e módulos de kernel. Suporta plataformas como Linux, BSD, Windows, AIX, Solaris e MacOS. Atua de forma centralizada, monitorando mudanças em diversas máquinas.

12

RESUMO

No caso do Linux, a própria distribuição Debian, recomendada para que cada um instale na máquina própria, provê o Snort já compilado, de modo que basta uma conexão com a internet e dois comandos para instalar a parte básica do Snort: apt-get update e apt-get install snort.O primeiro comando atualiza a base de pacotes do Debian e o segundo comando efetivamente instala a última versão do Snort disponível.

A configuração do Snort reside no arquivo /etc/snort/snort.conf. Esse arquivo é extenso e contém uma série de parâmetros de configuração do Snort.

Com o intuito de facilitar a atualização de regras, foi criada uma ferramenta chamada Oinkmaster, que permite que a atualização seja feita de forma automática. A instalação do Oinkmaster é automaticamente realizada junto com o Snort, durante a execução do comando apt-get install.

O Guardian é um script na linguagem Perl, que insere temporariamente regras de bloqueio em um firewall, a partir dos alertas gerados pelo Snort. Através do Guardian, a instalação de Snort passa a ter uma característica reativa.

O Snort-inline é um modo especial de funcionamento do Snort, integrado com o firewall Iptables/ netfilter para funcionar como um IPS. Cada pacote recebido pelo Iptables é encaminhado para uma fila (queue), para ser processado pelo Snort-inline, que pode descartar pacotes de acordo com as suas regras, de modo que o pacote não é passado adiante pelo processo de roteamento do firewall. Opcionalmente podem ser gerados registros e alertas correspondentes.

Outro projeto de IDS é o HLBR, desenvolvido no Brasil e disponível no sourceforge. O Bro IDS é um projeto open source de um sistema de detecção de intrusos baseado em rede. Forte concorrente do Snort, ele monitora de forma passiva o tráfego de rede em busca de atividades suspeitas. A sua análise inclui a detecção de ataques específicos (inclusive os definidos pelas assinaturas, mas também aqueles definidos em termos de eventos) e atividades incomuns (por exemplo, certo host conectar a determinados serviços ou falhas em tentativas de conexão).

Se o Bro detectar algo de interesse, pode ser configurado para gerar uma entrada de log, alertar o operador em tempo real, executar um comando do sistema operacional (por exemplo, para finalizar a conexão ou bloquear um host malicioso on-the-fly).