

IDS



<http://pplware.sapo.pt/wp-content/uploads/2009/09/snort1.jpg>



Índice

Índice	2
Apresentação	3
O que é um IDS	4
Entendendo melhor o funcionamento de um IDS	4
Características de um IDS	5
Vantagens de um IDS	5
O que é uma intrusão	6
Como detectar uma intrusão	6
Estrutura do IDS	7
Conhecendo o SNORT	10
Instalando o SNORT	11
Instalando o NMAP	12
Visualizando os logs do SNORT	13
Conclusão	14



Apresentação

Iniciamos aqui uma breve demonstração do funcionamento de um IDS. Esperamos que todos gostem e venham obter o máximo de conhecimento possível através deste material.

Em caso de dúvidas, envie as mesmas para: eudson@4psolucoes.com.br

Dos direitos autorais

Este material é o resultado de diversas fontes de pesquisa na internet e conhecimentos próprios, caso alguém veja conteúdo de sua autoria neste material e não teve seu nome citado favor informar em meu e-mail citado acima qual o conteúdo de sua autoria pois estarei providenciando os méritos neste material.

Esta apostila é de uso didático sem fins lucrativos. A mesma pode ser distribuída gratuitamente desde que sejam mantidos sua integridade de conteúdo.

Montagem e adaptação: Eudson Fonseca – eudsonbit1@gmail.com



O que é um IDS

UM IDS é uma ferramenta utilizada para detectar e alertar o administrador sobre ataques e tentativas de acesso indevidos na rede corporativa.

A Solução IDS é um conjunto de ferramentas que, aplicado ao **Firewall** proporciona o monitoramento do tráfego tanto de entrada quanto de saída das informações na rede.

FIREWALL → É utilizado para evitar que o tráfego não autorizado possa fluir de uma rede para outra. Apesar de se tratar de um conceito geralmente relacionado a proteção contra invasões, o *firewall* não possui capacidade de analisar toda a extensão do protocolo, ficando geralmente restrito ao nível 4 da camada OSI (Transporte).

Entendendo melhor o funcionamento de um IDS

Para facilitar o entendimento, vamos comparar um sistema IDS com o sistema de defesa do corpo humano.

Sistema de defesa do corpo humano

Os anticorpos constituem um mecanismo de defesa que o ser humano possui. Eles desempenham um importante papel na proteção do organismo contra substâncias estranhas.

Quando um vírus ou bactéria, por exemplo, invade o corpo humano, certos glóbulos brancos do sangue denominados linfócitos T, produzem e lançam na corrente sanguínea um tipo especial de proteína capaz de unir-se às moléculas que compõem este vírus ou bactéria, e assim inativando-o.

A proteína que o indivíduo produz, em resposta ao vírus ou bactéria, denomina-se anticorpo, e as substâncias estranhas, como vírus e bactérias, são denominadas antígenos.

Quando isso acontece nosso corpo então torna-se imune aquele vírus ou bactéria e se caso este vírus vier a invadir novamente o corpo já existirão anti-corpos específicos para eliminá-los.

Caso haja a invasão de um vírus desconhecido pelo corpo, então os linfócitos T se encarregarão de encontrar informações sobre esse novo vírus e criar uma vacina (anti-corpos) e eliminar este vírus, e é durante este período onde geralmente sentimos mal.

Sistema de IDS

O IDS, tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legítimo está fazendo mau uso do mesmo.

Esta ferramenta roda constantemente em *background* (*geralmente é recomendável um servidor só para este fim*) e somente gera uma notificação quando detecta alguma coisa que seja suspeita ou ilegal.

Assim sendo, podemos dizer que os linfócitos T corresponde aos sistemas de *firewalls*, *que sabem qual o tráfego pertence a rede de acordo com a configuração da política de rede*.

As imunidades são os padrões de ataques/assinaturas, ou seja, os ataques conhecidos previamente.

O sistema também é caracterizado por possuir inteligência para aprender com o comportamento da rede e, com isso, identificar novos padrões ou mutação dos padrões existentes. Este período de aprendizagem pode variar de acordo com o tráfego da rede.



Características de um IDS

Algumas características de um IDS são:

- ☑ O gerenciamento centralizado;
- ☑ Possibilidade de interação com outros elementos de rede como *firewall*, roteadores e consoles de gerência;
- ☑ A possibilidade de construir uma base de conhecimento centralizada de forma a permitir uma visão ampla do nível de segurança da rede e o conhecimento das ameaças existentes.

Desta forma, quando algum ataque (antígeno) for detectado pelo sistema, torna-se possível ações de conta-ataque (anticorpos) que podem ser:

- * Envio de *e-mail* para o administrador,
- * Envio de mensagem via *pager*,
- * Ativação de alertas nas estações de gerência via SNMP,
- * Reconfiguração de elementos de rede como *firewall* e roteadores, e até mesmo o encerramento da conexão através do envio de pacotes de *reset* (*flag* RST do TCP) para a máquina atacante e para a máquina atacada, com o objetivo de descarregar a pilha TCP.

Características de um IDS bem configurado

- ☞ Deve rodar continuamente sem interação humana e deve ser seguro o suficiente de forma a permitir sua operação em *background*; mas não deve ser uma caixa preta;
- ☞ Sua base de conhecimento não deve ser perdida quando o sistema for reinicializado, ou desligado inesperadamente;
- ☞ Deve monitorar a si próprio de forma a garantir sua segurança;
- ☞ Ter o mínimo de impacto no funcionamento do sistema;
- ☞ Poder detectar mudanças no funcionamento normal;
- ☞ Cada sistema possui padrões diferentes e a ferramenta de IDS deve ser adaptada de forma fácil aos diversos padrões;
- ☞ Cobrir as mudanças do sistema durante o tempo, como no caso de uma nova aplicação que comece a fazer parte do sistema;
- ☞ Ser difícil de ser enganado, por exemplo:
 - ☞ Quando a ferramenta classifica uma ação como uma possível intrusão, quando na verdade trata-se de uma ação legítima;
 - ☞ Quando uma intrusão real acontece e a ferramenta permite que ela passe como se fosse uma ação legítima;

Vantagens de um IDS

Através de um IDS podemos monitorar:

- ☞ Quais **serviços** estão sendo atacados;
- ☞ Qual a origem dos ataques;
- ☞ Portas e protocolos de acesso utilizados na tentativa de invasão;
- ☞ Softwares e **Backdoors** os quais o invasor tentou utilizar;
- ☞ Ocorrências adversas em geral;
- ☞ Acesso interno de sua rede a servidores IRC, ICQ, MSN, Yahoo Messenger;

Além de muitas Outras informações, as quais possibilitarão ao administrador da rede, manter-se sempre bem informado e prevenido.

SERVIÇOS → São serviços de rede em geral, como web, e-mail, proxy, firewall, etc.

BACKDOOR (Porta dos fundos) → É um programa de código fonte mal-intencionado que descobre e utiliza uma ou mais falhas de segurança para ter acesso ao sistema operacional. Partindo daí, gera uma "porta dos fundos" que pode ser inadvertidamente utilizada por terceiros para possíveis invasões.

O que é uma intrusão

Todas as intrusões estão definidas na política de segurança. Enquanto não for definido o que é permitido e o que não é permitido no sistema, é inútil tentar entender uma intrusão.

Uma intrusão pode ser definida como:

"Qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou do sistema."

Uma intrusão pode ser apurada a partir de parâmetros do sistema, como utilização da CPU, número de conexões por minuto, número de processos por usuário entre outros.

Uma variação significativa nestes padrões pode ser um indício de intrusão. Por exemplo, a exploração das vulnerabilidades de um sistema envolve a utilização indevida/anormal do sistema; então, podem ser descobertas violações de segurança a partir de padrões que fogem os padrões do uso do sistema.

O perigo pode estar "dentro de casa".

Muitos podem pensar que uma instituição está sujeita, na maior parte do tempo, a tentativas de invasão externas, ou seja, ataques originados de fora da instituição, geralmente da Internet.

No entanto, estudos revelam que a maior porcentagem de ataques tem origem dentro da própria instituição (intrusos internos), pois afinal:

- ✖ Quem poderia melhor conhecer a topologia da rede?
- ✖ Quem sabe onde os dados sensíveis estão armazenados e quais são os recursos de segurança disponíveis?

Levando-se em consideração o fato de que a maioria dos mecanismos de segurança são implementados com o objetivo de proteger a instituição dos ataques externos, muitos ataques ocorrem e muitas vezes não são notados; ou, quando o são, já é tarde demais.

Faz-se necessário, então, um mecanismo que detecte os dois tipos de ataque - uma tentativa externa ou interna.

Um sistema de IDS eficiente deve detectar os dois tipos de ataques.

Como detectar uma intrusão

Muitas ferramentas, de IDS realizam suas operações a partir da análise de padrões do sistema operacional e da rede tais como:

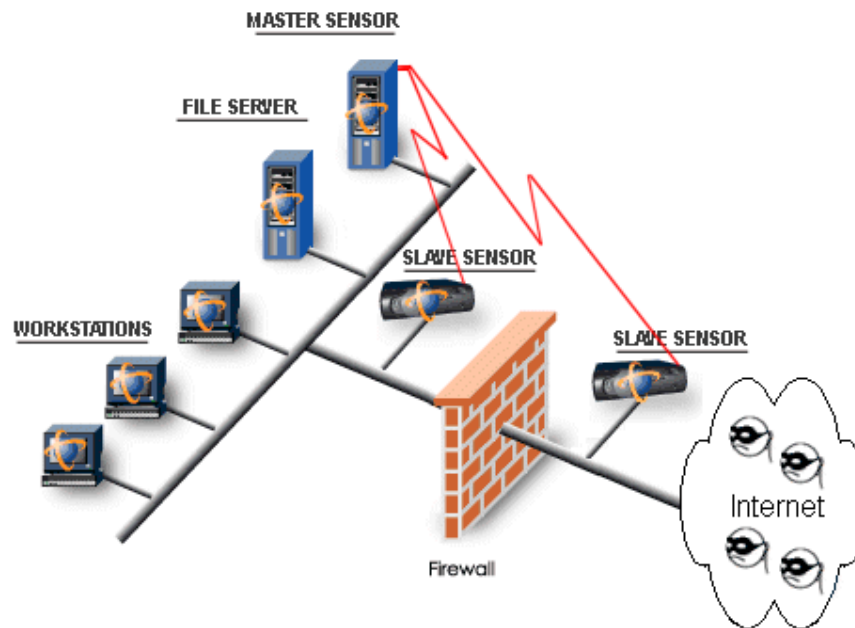
- ☞ Utilização de CPU;
- ☞ I/O de disco;
- ☞ Uso de memória;
- ☞ Atividades dos usuários;
- ☞ Número de tentativas de *login*;
- ☞ Número de conexões;
- ☞ Volume de dados trafegando no segmento de rede;
- ☞ Entre outros.

Estes dados formam uma base de informação sobre a utilização do sistema em vários momentos do tempo, outras já possuem bases com padrões de ataque previamente montadas permitindo também a configuração dos valores das bases bem como inclusão de novos parâmetros.

Com estas informações a ferramenta de IDS pode identificar as tentativas de intrusão e até mesmo registrar a técnica utilizada.

Estrutura de um IDS

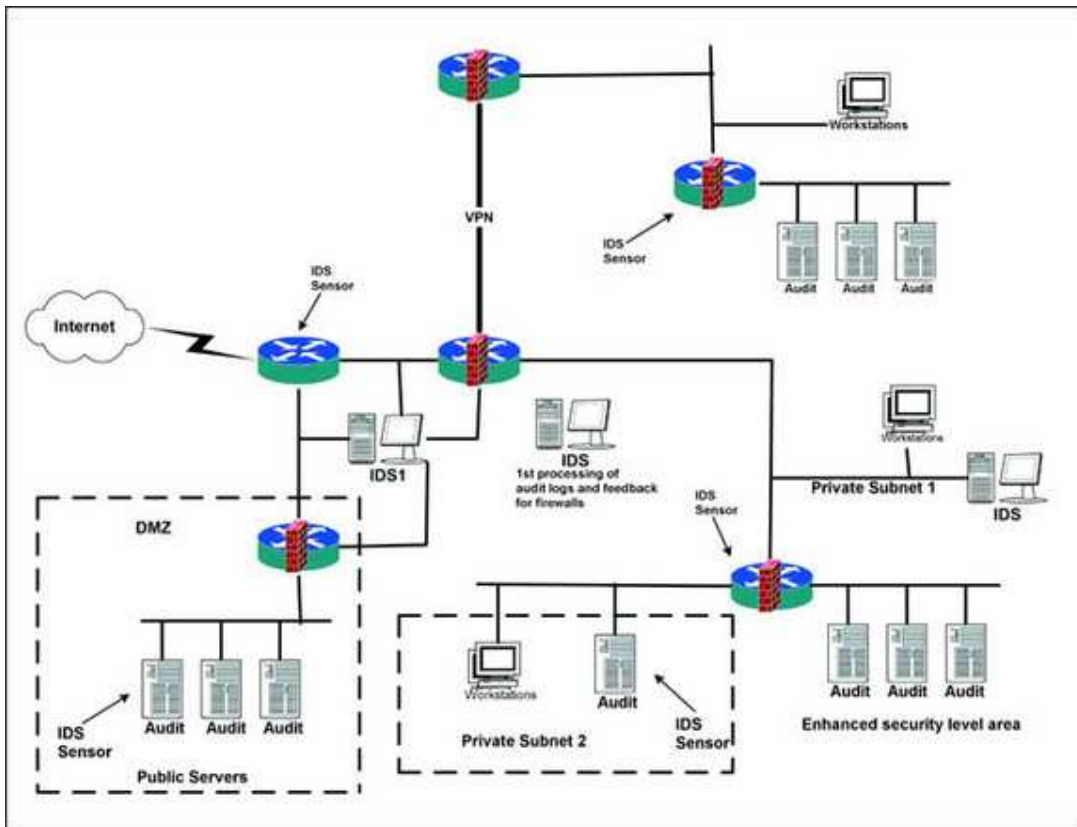
Neste exemplo, temos um servidor IDS monitorando o tráfego direto na internet, e, após o firewall, temos outro IDS monitorando o tráfego da rede.



http://ictlab.tyict.vtc.edu.hk/~tsangkt/reference/Silicon%20Defense%20-%20the%20cyber-war%20defense%20company_files/ids.gif



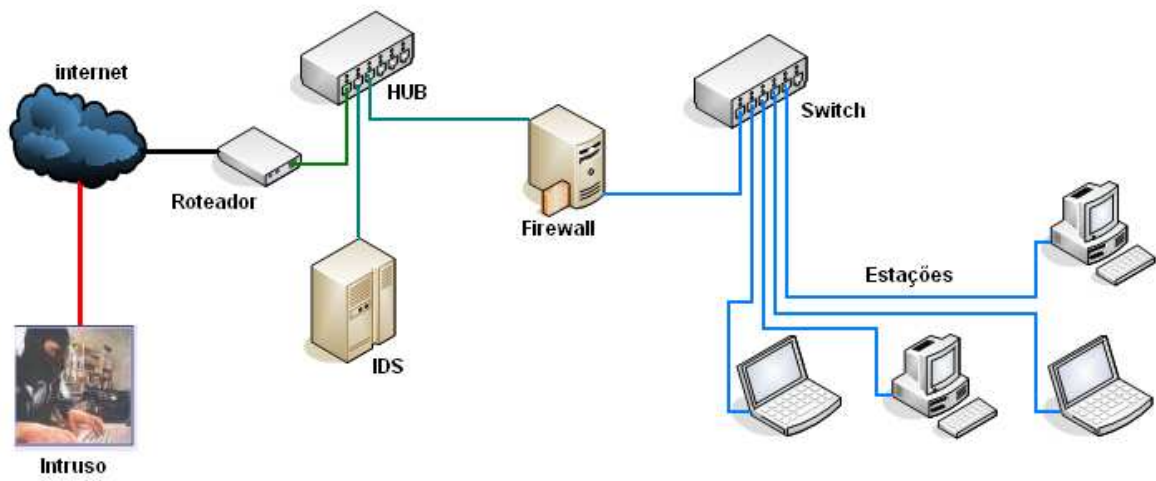
Neste outro exemplo, temos servidores IDS monitorando o tráfego vindo da internet e o tráfego interno.



http://www.windowsecurity.com/img/upl/Miejsce_IDS_Rys41034592917071.jpg



Para este exemplo, o servidor IDS monitorando o tráfego da rede interna e externa.



Conhecendo o SNORT

O Snort é um software livre de detecção de intrusão para rede (NIDS), capaz de desenvolver análise de tráfego em tempo real e registro de pacote em redes IP. Executa análise de protocolo, busca/associa padrões de conteúdo e pode ser usado para detectar uma variedade de ataques.

Esta ferramenta é suportada em arquiteturas RISC e CISC e em plataformas das mais diversas, como os vários sabores de Linux (RedHat, Debian, Slackware, Mandrake, etc.)

E também no Unix: OpenBSD, FreeBSD, NetBSD, Solaris, SunOS, HP-UX, AIX, IRIX, Tru64, MacOS X.

O Snort, desenvolvido por Martin Roesch, é um sistema peso leve de detecção de intrusão para rede, capaz de desenvolver análise de tráfego em tempo real e registro de pacote em redes IP. Executa análise de protocolo, busca/associa padrões de conteúdo e pode ser usado para detectar uma variedade de ataques, tais como buffer overflows, stealth port scans, ataques CGI, SMB probes, OS fingerprinting, entre outras.

Neste sistema utiliza-se, uma linguagem de regras flexível para indicar o tráfego que será coletado ou passará, assim como um engenho de detecção que utiliza uma arquitetura plug-in modular.

Uma característica relevante é a capacidade de gerar alertas em tempo real, que incorpora mecanismos de alerta para o syslog, para arquivo, para socket UNIX ou, com auxílio do SAMBA (smbclient), para o WinPopup messages em máquinas Windows clientes.

Por ser uma ferramenta peso leve, a utilização do Snort é indicada para monitorar redes TCP/IP pequenas, onde pode detectar uma grande variedade do tráfego suspeito, assim como ataques externos e então, fornece argumento para as decisões dos administradores.

Fontes: Wikipedia, UFSC

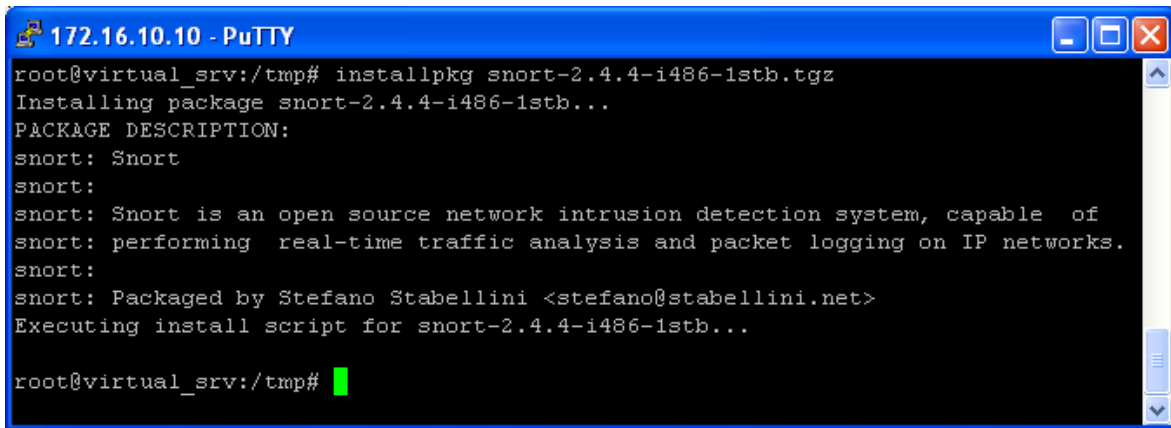


www.4psolucoes.com.br

Instalando o SNORT

Primeiramente devemos baixar e instalar o pacote do snort, o link abaixo leva direto ao download da versão 2.4 para Slackware, a figura abaixo mostra o comando de instalação:

<http://www2.linuxpackages.net/packages/Slackware-10.2/Daemon/snort/snort-2.4.4-i486-1stb.tgz>



```
172.16.10.10 - PuTTY
root@virtual_srv:/tmp# installpkg snort-2.4.4-i486-1stb.tgz
Installing package snort-2.4.4-i486-1stb...
PACKAGE DESCRIPTION:
snort: Snort
snort:
snort: Snort is an open source network intrusion detection system, capable of
snort: performing real-time traffic analysis and packet logging on IP networks.
snort:
snort: Packaged by Stefano Stabellini <stefano@stabellini.net>
Executing install script for snort-2.4.4-i486-1stb...

root@virtual_srv:/tmp#
```

O próximo passo será a configuração do snort, o arquivo de configuração do mesmo encontra-se em /etc e se chama snort.conf

O comando abaixo acessa o arquivo para configuração:

```
vi /etc/snort.conf
```

Após o snort ter sido configurado a rede em que ele atuará e o DNS, devemos iniciar o mesmo com o seguinte comando:

```
snort -D
```

* A opção "-D" indica que o snort rodará em background.



```
172.16.10.10 - PuTTY
root@virtual_srv:/tmp# snort -D
root@virtual_srv:/tmp#
```



Instalando o NMAP

Logo depois do snort estar rodando qualquer tentativa de intrusão será detectado pelo mesmo e armazenado em um arquivo de log. Vamos fazer um teste usando um scanner de portas muito conhecido chamado nmap, que é um escaneador de hosts que usa recursos avançados para verificar o estado do seu alvo. A ferramenta é gratuita e encontrada nas versões Linux, Windows(95,98,NT, Me, 2K e XP), Mac OS, Solaris, FreeBSD e OpenBSD.

Este software foi desenvolvido para scanear redes extensas rapidamente, embora trabalhe melhor com hosts únicos. O nmap é capaz de determinar quais hosts estão disponíveis na rede, quais serviços estão oferecendo, qual sistema operacional está rodando, qual tipo de pacote de filtro / firewall estão usando, e uma dúzia de outras características.

Para obter o Nmap, basta entrar no seguinte site: http://www.insecure.org/nmap/nmap_download.html.

Neste site você encontrará as versões para Linux e para Windows, sendo que a versão do Windows exige a instalação de algumas bibliotecas, estas bibliotecas também estão presentes no site citado, bastando realizar também o download do aplicativo WinPcap.

Para usar o nmap tanto em Windows quanto em Linux os comandos praticamente são os mesmos, no Windows, para um scan básico basta acessar a pasta onde ele está armazenado e digitar o seguinte comando:

```
nmap -O <ip_do_alvo>
```

Desta maneira ele irá escanear o servidor alvo mostrando as portas abertas e a versão do sistema operacional que roda no mesmo (-O).

```

C:\WINDOWS\system32\cmd.exe

C:\nmap>nmap -O 172.16.10.10

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2006-10-03 22:32 Hora ofi
cial do Brasil
Interesting ports on 172.16.10.10:
(The 1657 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
37/tcp    open  time
80/tcp    open  http
113/tcp   open  auth
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:03:FF:CF:25:5B (Microsoft) Endereço MAC do Servidor
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 0.206 days (since Tue Oct 03 17:35:14 2006)

Nmap finished: 1 IP address (1 host up) scanned in 5.047 seconds

C:\nmap>_
  
```



Visualizando os logs do SNORT

```
root@virtual_srv:~# cat /var/log/snort/alert

[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/10-23:27:22.892685 172.16.2.2 -> 172.16.10.10
ICMP TTL:50 TOS:0x0 ID:27465 IpLen:20 DgmLen:28
Type:8 Code:0 ID:49012 Seq:26234 ECHO
[Xref => http://www.whitehats.com/info/IDS162]
```

```
[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
03/10-23:27:22.892685 172.16.2.2 -> 172.16.10.10
ICMP TTL:50 TOS:0x0 ID:27465 IpLen:20 DgmLen:28
Type:8 Code:0 ID:49012 Seq:26234 ECHO
```

```
[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
03/10-23:27:22.892766 172.16.10.10 -> 172.16.2.2
ICMP TTL:64 TOS:0x0 ID:6500 IpLen:20 DgmLen:28
Type:0 Code:0 ID:49012 Seq:26234 ECHO REPLY
```

```
[**] [122:1:0] (portscan) TCP Portscan [**]
03/10-22:27:22.939639 172.16.2.2 -> 172.16.10.10
PROTO255 TTL:0 TOS:0x0 ID:0 IpLen:20 DgmLen:156 DF
```

```
[**] [1:1228:7] SCAN nmap XMAS [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/10-22:27:25.079541 172.16.2.2:39573 -> 172.16.10.10:1
TCP TTL:45 TOS:0x0 ID:59960 IpLen:20 DgmLen:60
**U*P**F Seq: 0x4D2E73A5 Ack: 0x0 Win: 0x800 TcpLen: 40 UrgPtr: 0x0
TCP Options (5) => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL
[Xref => http://www.whitehats.com/info/IDS30]

** END OF DUMP
```



Conclusão

Como qualquer outro curso, principalmente On-Line são os próprios alunos que fazem a diferença, os resultados vem do esforço e dedicação de cada um, nós da equipe da 4P Soluções estamos muito honrados em lhe repassar um pouco do que sabemos, e esperamos que com esse pouco você possa fazer muito.

Com os conhecimentos adquiridos aqui você já estará apto a iniciar suas implementações de servidores IDS, porém não se esqueça que o conteúdo proposto aqui é só o início, há muito o que estudar e aprender ainda. Porém quem quer consegue, sabemos que não é fácil e a caminhada é longa, mas a recompensa é garantida.

Ajude-nos a manter nosso mini-curso sempre com uma boa qualidade de aprendizado, envie-nos sua opinião, reclamação ou sugestão para eudson@4psolucoes.com.br

Muito obrigado,
Eudson Fonseca.

