Detecção de Intrusos

Rodrigo Rubira Branco
rodrigo@firewalls.com.br

FIREWALLS SECURITY

(nfr)(security)

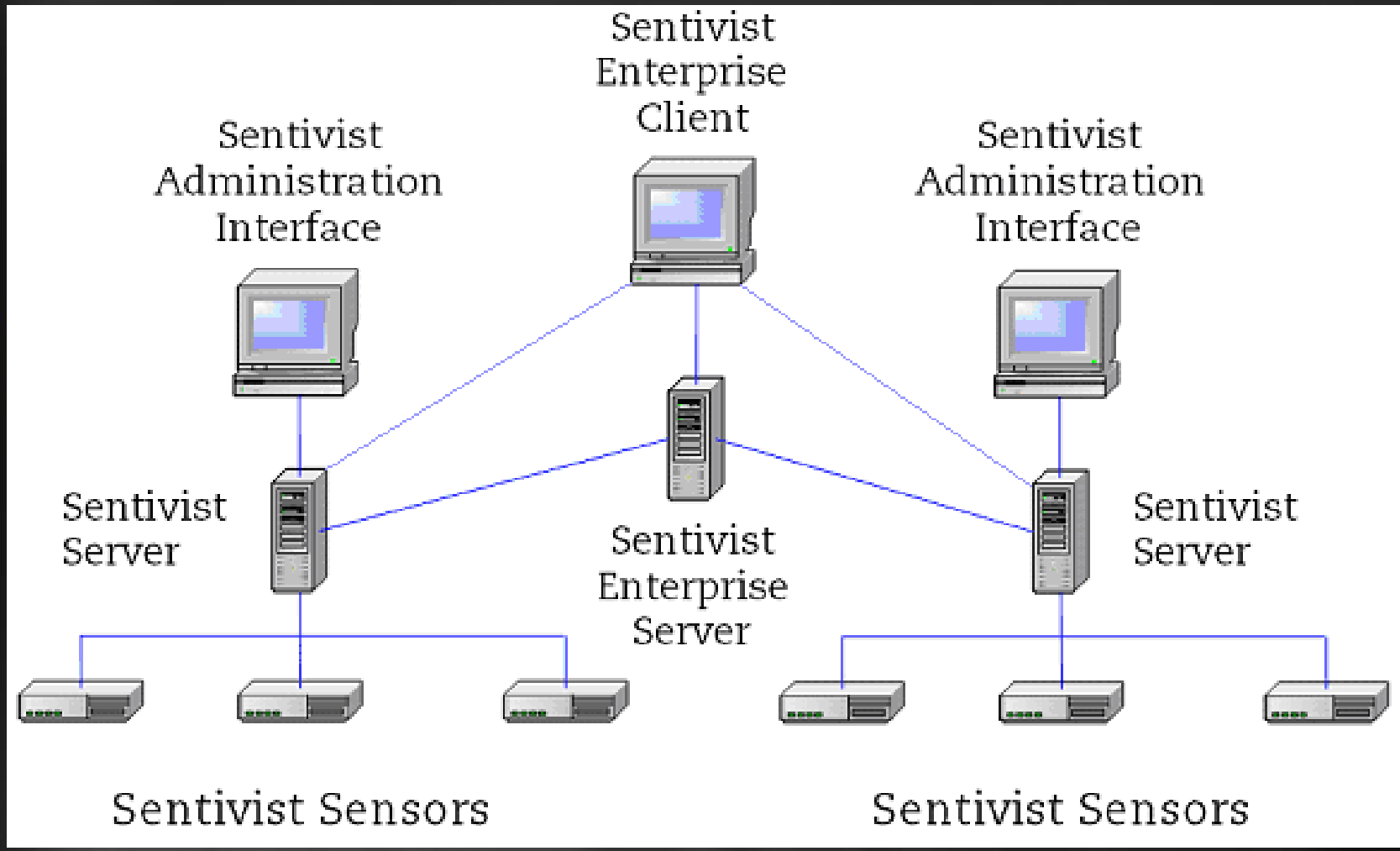
Firewalls - Sumário

- Empresa Especializada em Segurança.
- Profissionais Certificados.
- Atenta a Padrões Internacionais.
- Parceira das maiores empresas de Segurança do Mundo.
- Visão de Negócios e Ética Empresarial.
- Soluções Personalizadas para a Realidade das Empresas.

NFR - Sumário

- Empresa Especializada em Detecção e prevensão de intrusos.
- Diversas Certificações – OSEC, OPSEC, CC.
- Presença Internacional.
-Compatibilidade com produtos renomados (Checkpoint, IBM/Tivoli, HP/OpenView) .
- Time de Resposta Altamente Eficaz.

Arquitetura do NFR



Objetivos

- Explicar os fundamentos de detecção de intrusos.
- Demonstrar a importância do reconhecimento de assinaturas de ataques.
- Apresentar as dificuldades existentes em detecção de intrusão.
- Fornecer formas de se analizar assinaturas de ataques.
- Demonstrar possibilidades existentes em detecção de intrusão.

Conceitos

CIDAL

Confidencialidade
Integridade
Disponibilidade
Autenticidade
Legalidade

LEMBRAR-SE SEMPRE DISTO NO DECORRER DA PALESTRA!

(nfr)(security)

Ambiente

Trabalhamos em um mundo real de sistemas mal configurados:

- **Bugs de Software;**
- **Empregados Insatisfeitos;**
- **Administradores de Sistemas Sobrecarregados;**
- **Acomodação de necessidades empresariais;**
- **Falta de Educação em Segurança;**
- **B2B,B2C,B2E,C2C,X2X ?**

Defense In-Depth

- **Um Firewall apenas aumenta o nível de segurança.**
- **O conceito de segurança em camadas garante que as falhas existentes em um Firewall sejam supridas por outros tipos de defesa e segurança.**
- **Através de diversas camadas cria-se um modelo de segurança robusto e capaz de suportar falhas.**

Quando pensar em Segurança pense em uma CEBOLA.

(nfr)(security)

Por que utilizar?

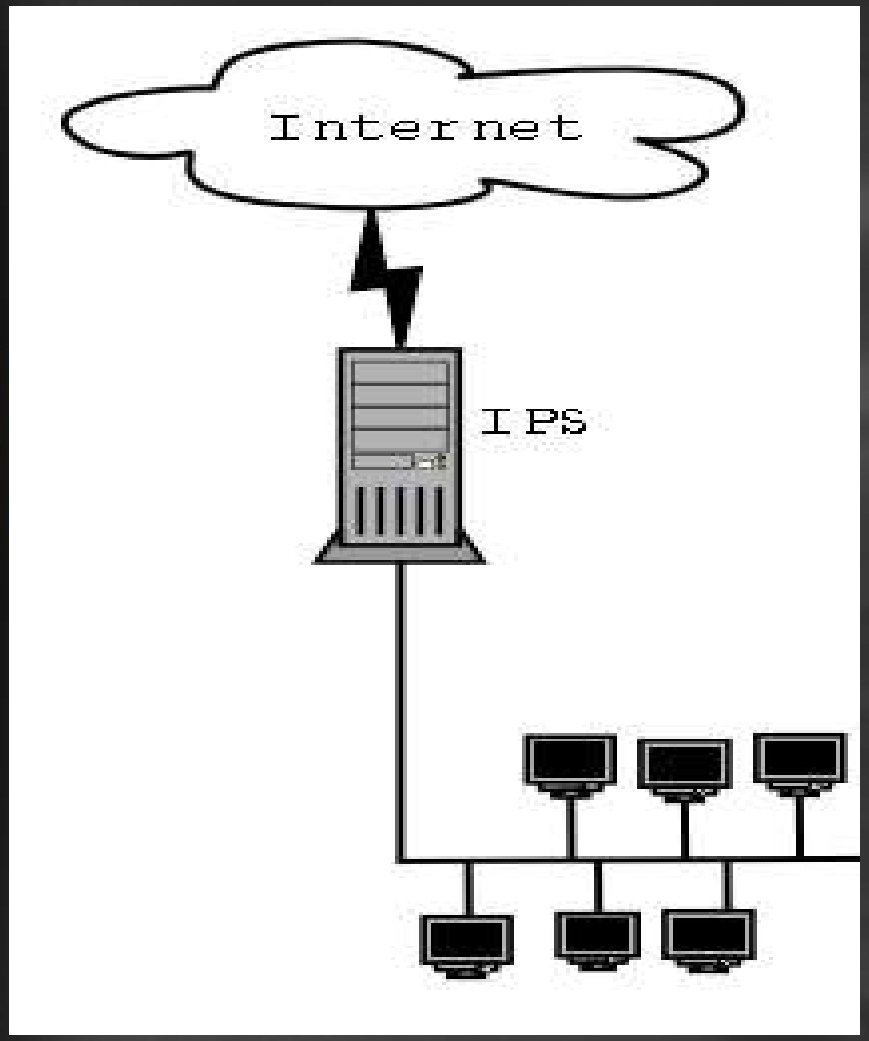
- **Firewalls podem agir somente sob ataques, IDS detectam as varreduras.**
- **Firewalls agem segundo regras pré-estabelecidas que geralmente não enxergam a camada de aplicação.**

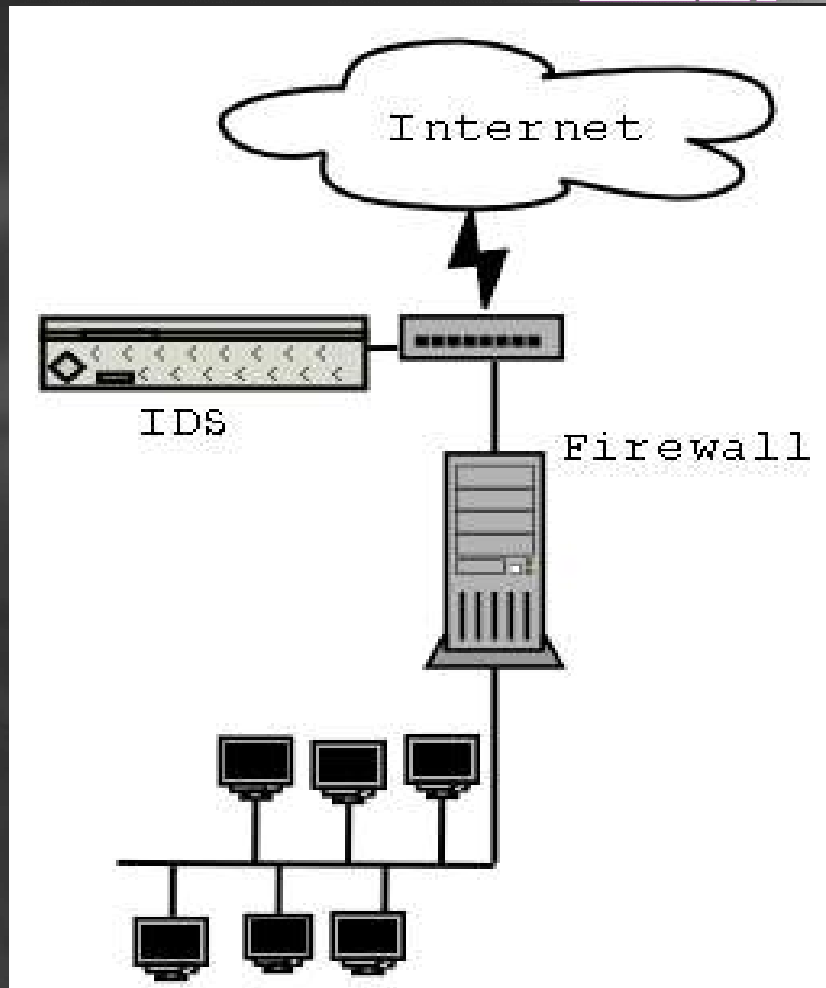
Por que utilizar?

Por que utilizar?

(nfr)(security)

IDS x IPS





Tipos de IDS

Constitui-se de 4 grandes tipos, a saber:

- **HIDS**
- **NIDS**
- **IDS Ativo**
- **IDS Passivo**

Baseados em:

- **Assinaturas**
- **Eventos**

Fornecedores

- NFR
- Sourcefire
- Snort
- Securepoint
- Cisco
- Symantec
- CA
- ISS

Assinaturas de Ataques

- **Todo ataque possui caracteristicas ÚNICAS que permitem distinguí-lo de outros ataques e principalmente do tráfego normal da rede.**

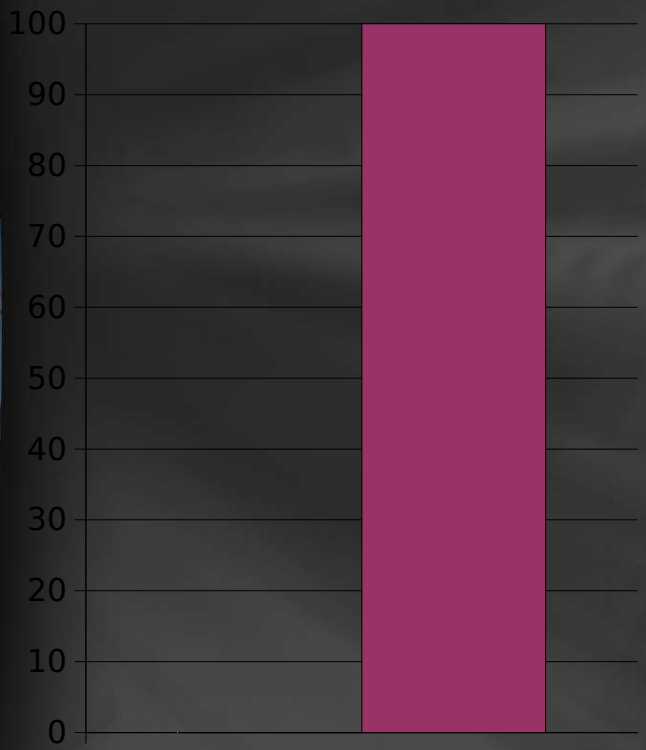
- **Tais caracteristicas são chamadas de Assinaturas de Ataques.**

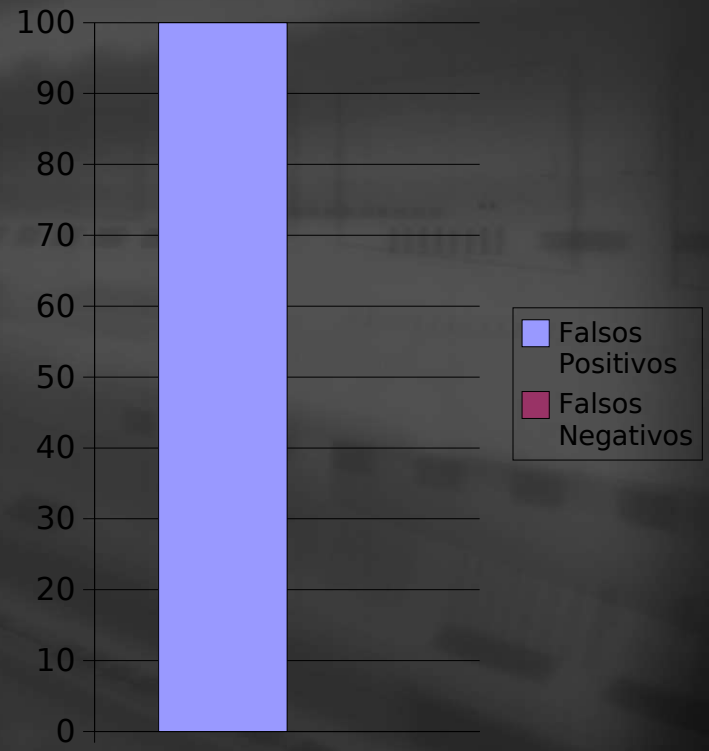
Assinaturas de Ataques

Problemas

- Fragmentação;
- Criptografia (VPN);
- UUEncode/Gzip Encode;
- Velocidade dos Links;
- Assinaturas baseadas em “pattern match”, ou seja, reconhecimento de determinada string dentro de um determinado pacote;
- Consolidação e correlação;
- Mantimento de sessões;
- Técnicas de polimorfismo;
- “Falhas” em sensores;
- Falsos Positivos x Falsos Negativos x Falsas Interpretações.

Positivos x Negativos





(nfr)(security)

Soluções

- **Diminuir falsos positivos integrando com analise de vulnerabilidades**

- **VANTAGENS x DESVANTAGENS**

- **- Automatizando o processo**
- **- Inteligencia em Deteccao**
- **- Gerenciamento integrado de detectores**
- **- Correlacao de eventos e sua importancia**
- **- Integracao com Firewalls**

Exposição x Vuln

- **Vulnerabilidade**

  Existência de determinada falha de segurança que pode ser explorada, dando acesso a execução de códigos arbitrários ou informações confidenciais.

- **Exposição**

  Existência de determinada má configuração de sistema, que permite coleta de informações. Chamamos de exposição qualquer tipo de configuração de segurança não adequada.

Ex: Um servidor de DNS que permite transferência de zonas.

(nfr)(security)

Origem de um Ataque

Quando topamos com determinado ataque, devemos precisar sua origem. Esta pode ser:

- **Real**
- **“Spoofada”**
- **Efeito colateral**

Ataques polimorficos?

- Consiste em ataques que se auto-decodificam durante a execução no sistema alvo.
- Evitam análises do tipo “pattern-matching”
- Impossíveis de serem detectados, causam problemas em assinaturas genéricas.
- Assinaturas Genéricas: Visam detectar todo tipo de ataque que possua uma caracteristica comum, por exemplo NOPs em instruções assembly.

0 DAY x Polimorfismo

- Impossível o uso de Técnicas utilizadas pelos Antivirus, devido a necessidade de análise em tempo real.
- Talvez a criação de assinaturas baseadas em serviços, porém não detectariam ataques 0 DAY.
- SCMorphism -> Ferramenta para testes de detectores de intrusos contra técnicas polimorficas.

Mecanismos de Ataque

Antes de escrevermos uma assinatura de ataque, precisamos de alguns conhecimentos basicos sobre o que desejamos:

- **Estímulo ou resposta?**
- **Serviço alvo**
- **Existe vulnerabilidade ou exposição pública ao serviço?**
- **Tráfego normal, exploração, DoS ou reconhecimento?**
- **Dispositivos auxiliares de informação (Firewalls, roteadores, sistemas)**

IDS + Traffic Shaping

- **Controle de DoS, Worms e Virus**
- **Controle de Spams, e uso de link por aplicativos indevidos**
- **Garantia de disponibilidade dos servicos essenciais**

Severidade

- As assinaturas de um ataque podem ser mais específicas ou genéricas.

- A severidade de um ataque pode facilmente ser vista de simples fatos:
  - O scan foi lançado contra toda a rede ou contra uma máquina específica?
  - A máquina específica a qual o scan foi lançado possuia o serviço requisitado ou foi feita uma busca por todos os serviços?
  - A busca específica ao recurso foi feita por uma versão específica ou tentou-se descobrir a versão?
  - Houve um resultado a despeito da busca efetuada?

Exemplo 1: DNS

[**] [1:1616:6] DNS named version attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-02:36:53.489089 192.168.0.10:1041 -> 192.168.0.11:53
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:58 DF
Len: 30

[**] [1:255:12] DNS zone transfer TCP [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-11:32:58.584907 192.168.0.10:1052 -> 192.168.0.1:53
TCP TTL:64 TOS:0x2 ID:53804 IpLen:20 DgmLen:72 DF
AP Seq: 0x4F5E4B1 Ack: 0xE4D61682 Win: 0x16D0 TcpLen: 20

[**] [1:624:6] SCAN SYN FIN [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-03:37:43.085849 192.168.0.11:10004 -> 192.168.0.10:53
TCP TTL:255 TOS:0x0 ID:2304 IpLen:20 DgmLen:40
******SF Seq: 0x56F2CD88 Ack: 0x0 Win: 0x1000 TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS198]

Exemplo 1: DNS

[**] [1:256:5] DNS named authors attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-02:40:31.425495 192.168.0.11:32848 -> 192.168.0.10:53
UDP TTL:64 TOS:0x0 ID:2746 IpLen:20 DgmLen:58 DF
Len: 30

SEVERIDADE = (CRITICIDADE + LETALIDADE) – (DEFESAS SISTEMA + DEFESAS REDE)

CRITICIDADE = 5 (DNS)
LETALIDADE = 2 (LEVANTAMENTO DE INFOS)
DEFESAS SISTEMA = 4 (SO ATUALIZADO E MODERNO)
DEFESAS REDE = 1 (FIREWALL DEIXOU PASSAR)

- SE FOI SUCEDIDO, SOMAR 1 A SEVERIDADE TOTAL

Exemplo 2: WEB

[**] [1:1260:11] WEB-MISC long basic authorization string [**]
[Classification: Attempted Denial of Service] [Priority: 2]
11/04-02:36:16.731399 192.168.0.10:1065 -> 192.168.0.11:80
TCP TTL:64 TOS:0x0 ID:29020 IpLen:20 DgmLen:1500 DF
A* Seq: 0x8AA2EA40 Ack: 0x507F49DB Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 629685 620484

[**] [1:498:6] ATTACK-RESPONSES id check returned root [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/04-01:34:25.713398 192.168.0.10:61200 -> 192.168.0.11:32790
TCP TTL:64 TOS:0x0 ID:41757 IpLen:20 DgmLen:91 DF
AP Seq: 0x791C8E50 Ack: 0x3FA7E3AD Win: 0x16A0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 601366 592250

Exemplo 3: DDoS

[**] [1:236:6] DDOS Stacheldraht client check gag [**]
[Classification: Attempted Denial of Service] [Priority: 2]
11/04-03:37:38.975728 192.168.0.11 -> 192.168.0.10
ICMP TTL:64 TOS:0x0 ID:13330 IpLen:20 DgmLen:39
Type:0 Code:0 ID:668 Seq:1 ECHO REPLY

[**] [1:239:2] DDOS shaft handler to agent [**]
[Classification: Attempted Denial of Service] [Priority: 2]
11/04-03:37:41.892842 192.168.0.11:1024 -> 192.168.0.10:18753
UDP TTL:255 TOS:0x0 ID:2304 IpLen:20 DgmLen:49
Len: 21
[Xref => http://www.whitehats.com/info/IDS255]

Exemplo 3: DDoS

[**] [1:221:4] DDOS TFN Probe [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-03:37:57.067216 192.168.0.11 -> 192.168.0.10
ICMP TTL:255 TOS:0x0 ID:2304 IpLen:20 DgmLen:32
Type:8 Code:0 ID:678 Seq:1 ECHO

[**] [1:245:3] DDOS mstream handler ping to agent [**]
[Classification: Attempted Denial of Service] [Priority: 2]
11/04-02:41:07.652728 192.168.0.11:65535 -> 192.168.0.10:10498
UDP TTL:255 TOS:0x0 ID:2304 IpLen:20 DgmLen:33
Len: 5

[**] [1:237:2] DDOS Trin00 Master to Daemon default password attempt [**]
[Classification: Attempted Denial of Service] [Priority: 2]
11/04-02:40:36.249665 192.168.0.11:1024 -> 192.168.0.10:27444
UDP TTL:255 TOS:0x0 ID:2304 IpLen:20 DgmLen:39
Len: 11
[Xref => http://www.whitehats.com/info/IDS197]

Exemplo 4: Compartilhamento

[**] [1:2466:4] NETBIOS SMB-DS IPC$ share unicode access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
11/04-11:19:03.222122 192.168.0.10:1050 -> 192.168.0.11:445
TCP TTL:64 TOS:0x0 ID:24752 IpLen:20 DgmLen:146 DF
AP Seq: 0xD25D9205 Ack: 0x9C265F80 Win: 0x1920 TcpLen: 32
TCP Options (3) => NOP NOP TS: 258110 262608

[**] [1:648:7] SHELLCODE x86 NOOP [**]
[Classification: Executable code was detected] [Priority: 1]
11/04-02:46:06.489881 192.168.0.1:139 -> 192.168.0.10:1038
TCP TTL:69 TOS:0x10 ID:53072 IpLen:20 DgmLen:1279 DF
AP Seq: 0x473A207B Ack: 0x298CE1BF Win: 0xF53C TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

Exemplo 5: SNMP

[**] [1:1418:11] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-03:37:29.755834 192.168.0.11:34037 -> 192.168.0.10:161
TCP TTL:64 TOS:0x0 ID:91 IpLen:20 DgmLen:60 DF
******S* Seq: 0x2FFF0490 Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 984267 0 NOP WS: 0

[**] [1:1420:11] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-03:37:29.755984 192.168.0.11:34038 -> 192.168.0.10:162
TCP TTL:64 TOS:0x0 ID:45558 IpLen:20 DgmLen:60 DF
******S* Seq: 0x3075B53D Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 984267 0 NOP WS: 0

[**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-03:37:29.969789 192.168.0.11:34581 -> 192.168.0.10:705
TCP TTL:64 TOS:0x0 ID:16370 IpLen:20 DgmLen:60 DF
******S* Seq: 0x2F7D3B12 Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 984288 0 NOP WS: 0

Exemplo 5: SNMP

[**] [1:1411:10] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-02:41:52.608935 192.168.0.10:1041 -> 192.168.0.11:161
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:73 DF
Len: 45

[**] [1:1417:9] SNMP request udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/04-02:41:52.608935 192.168.0.10:1041 -> 192.168.0.11:161
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:73 DF
Len: 45

Certificação OSEC

- Para sistemas de IDS e Firewall (OSEC)
- Mantido por um laboratorio Neutro: www.neohapsis.com
- Testes de fragmentacao/segmentacao (altas velocidades)
- Testes com grandes numeros de sessoes e de estado
- Teste de integridade e de base de assinaturas
- Testes de descarte de pacotes manipulados/forjados
- Testes de injecao de delay e ofuscacao HTTP
- Injecao de Strings

Certificação OPSEC

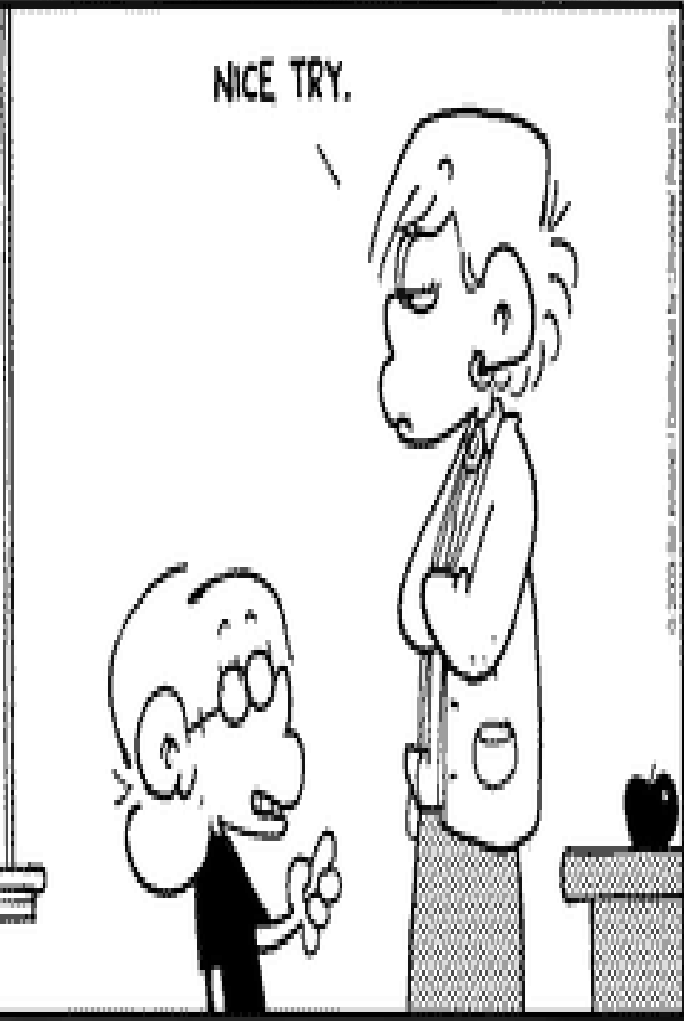
- Para sistemas de Seguranca se Integrarem
- Consorcio liderado pela Checkpoint
- Teste de integracao
- Testes de gerenciamento

Quem implementaria?

```
#include <stdio.h>
int main(void)
{
   int count;

   for (count = 1; count <= 500; count++)
      printf("I will not throw paper airplanes in class.");

   return 0;
}
```



Legalidade

- Direito a Privacidade (intimidade)
- Informacoes particulares podem ser capturadas?
- Convencendo Diretores/Funcionarios
- Termo aditivo ao contrato de trabalho

Referências

- SCMorphism

  http://www.bsdaemon.org

- SANS

  http://www.sans.org

- Security Focus

  http://www.securityfocus.com

- NFR Security

  http://www.nfr.com

- ISS

  http://www.iss.net

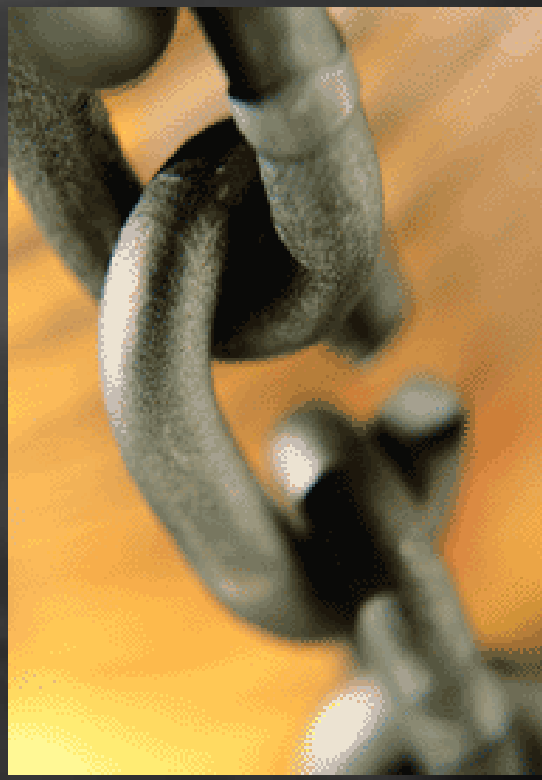
(nfr)(security)

Agradecimentos

- Eventos, Workshops, Seminários, Palestras, RoadShows, Conversas

- Comunicação

- Elo mais fraco da segurança da informação



(nfr)(security)

DÚVIDAS ?

Rodrigo Rubira Branco
rodrigo@firewalls.com.br

(nfr)(security)