Defeating Security Systems

Polymorphism x SandBox
SCMorphism x Checkpoint

Rodrigo Rubira Branco
rodrigo@firewalls.com.br
bsdaemon@bsdaemon.org

Abstract

When i have talked about polymorphic attacks and my scmorphism tool (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!

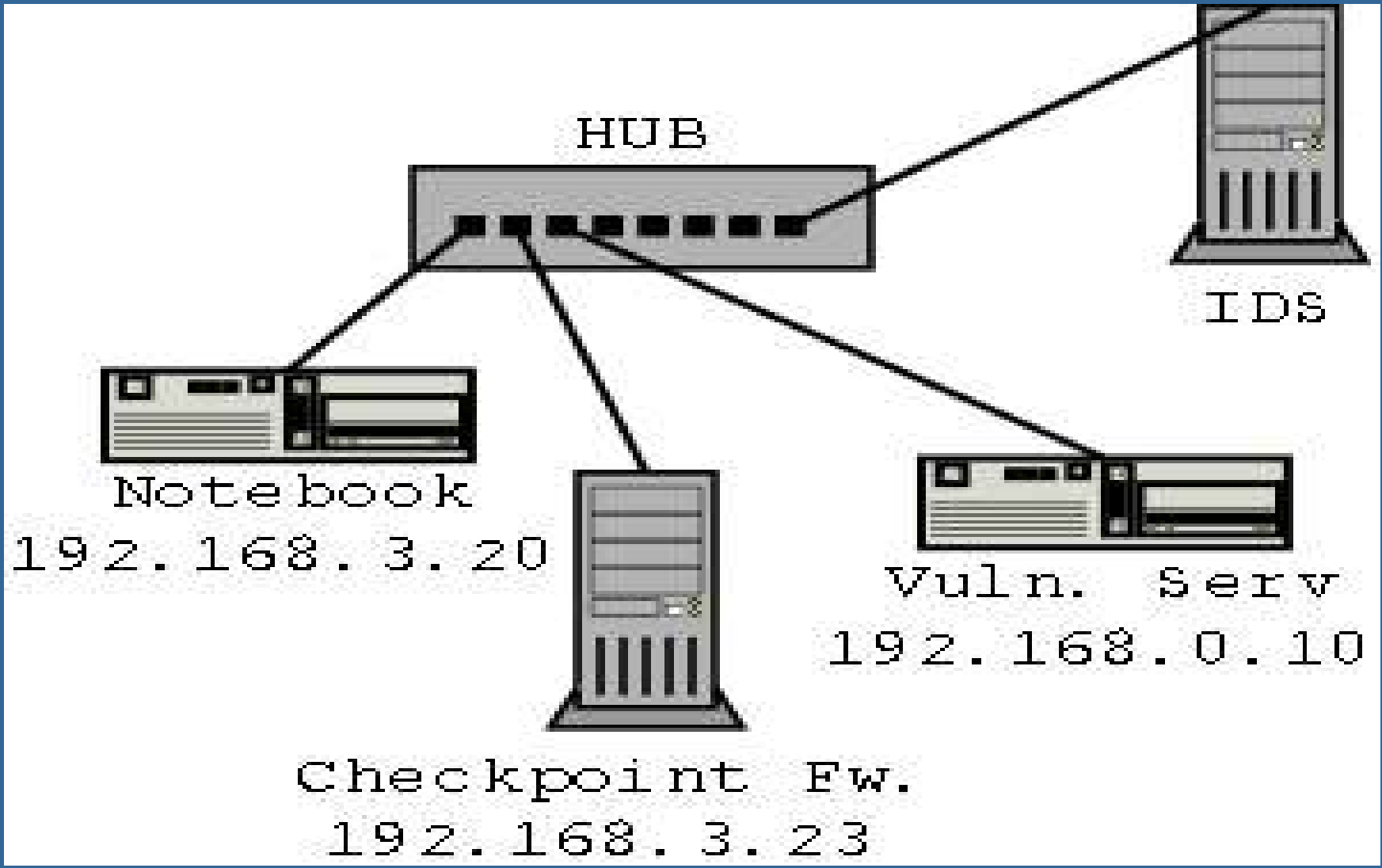
Notice

"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) to share with me all machines and software needed to test and to give to me, my work time to study polymorphic attacks."

The LAB.


HUB
IDS
Notebook
192.168.3.20
Vuln. Serv
192.168.0.10
Checkpoint Fw.
192.168.3.23

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.

Confs.

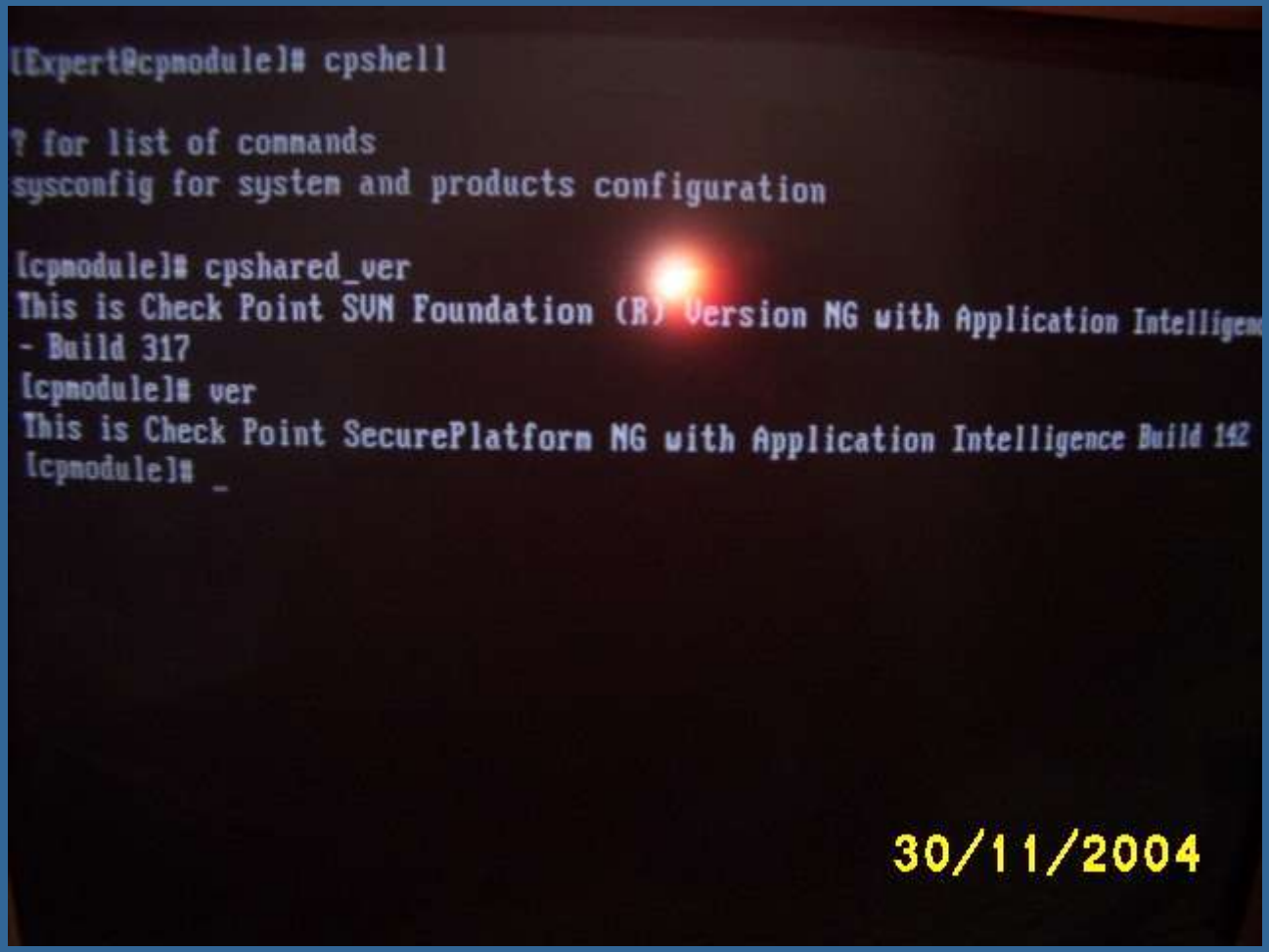
Notebook Configuration: gateway and network

Checkpoint

Checkpoint Configuration: Gateway and Network

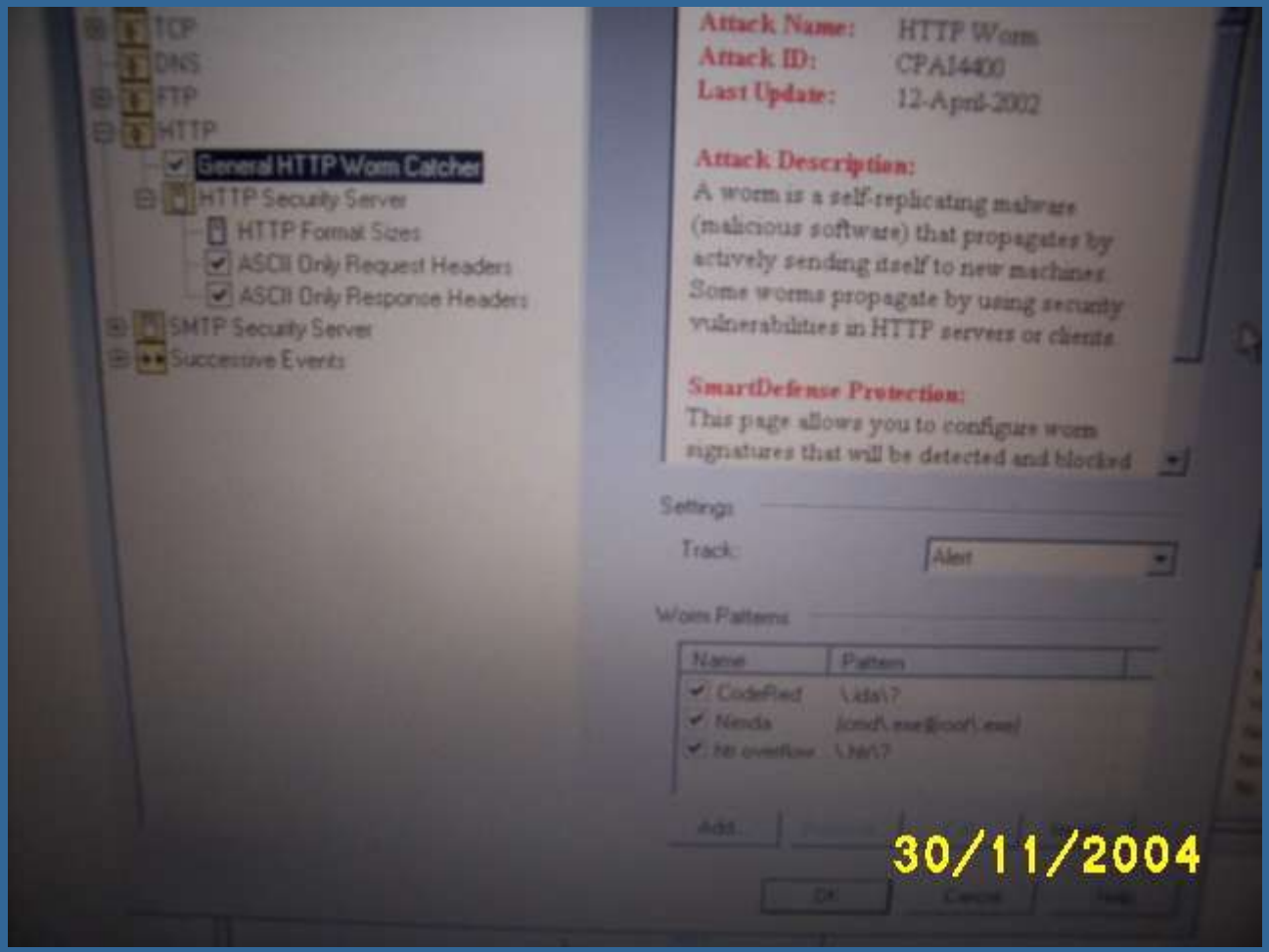
Checkpoint

Checkpoint Version Information



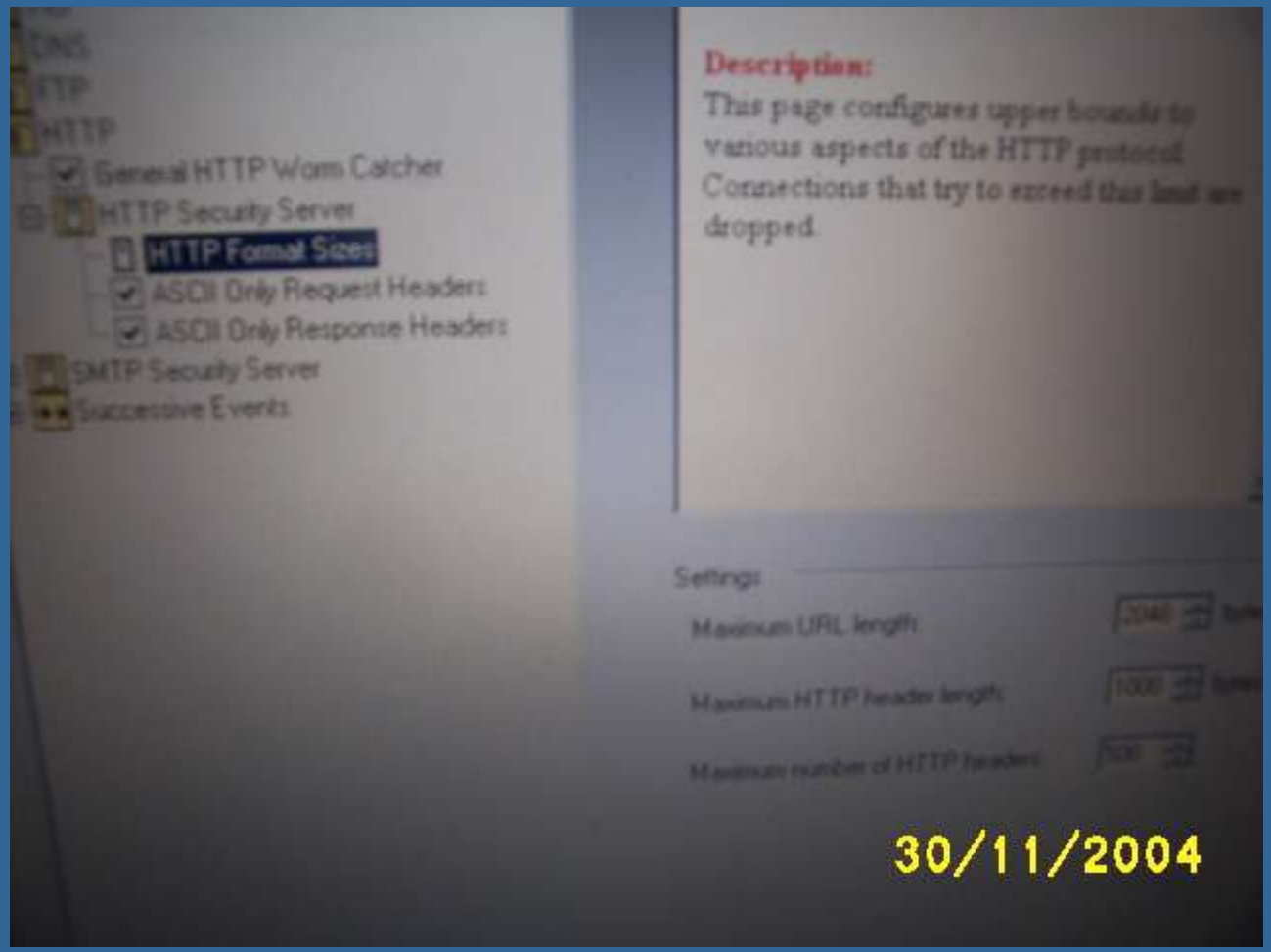
Checkpoint

Smart Defense HTTP Options



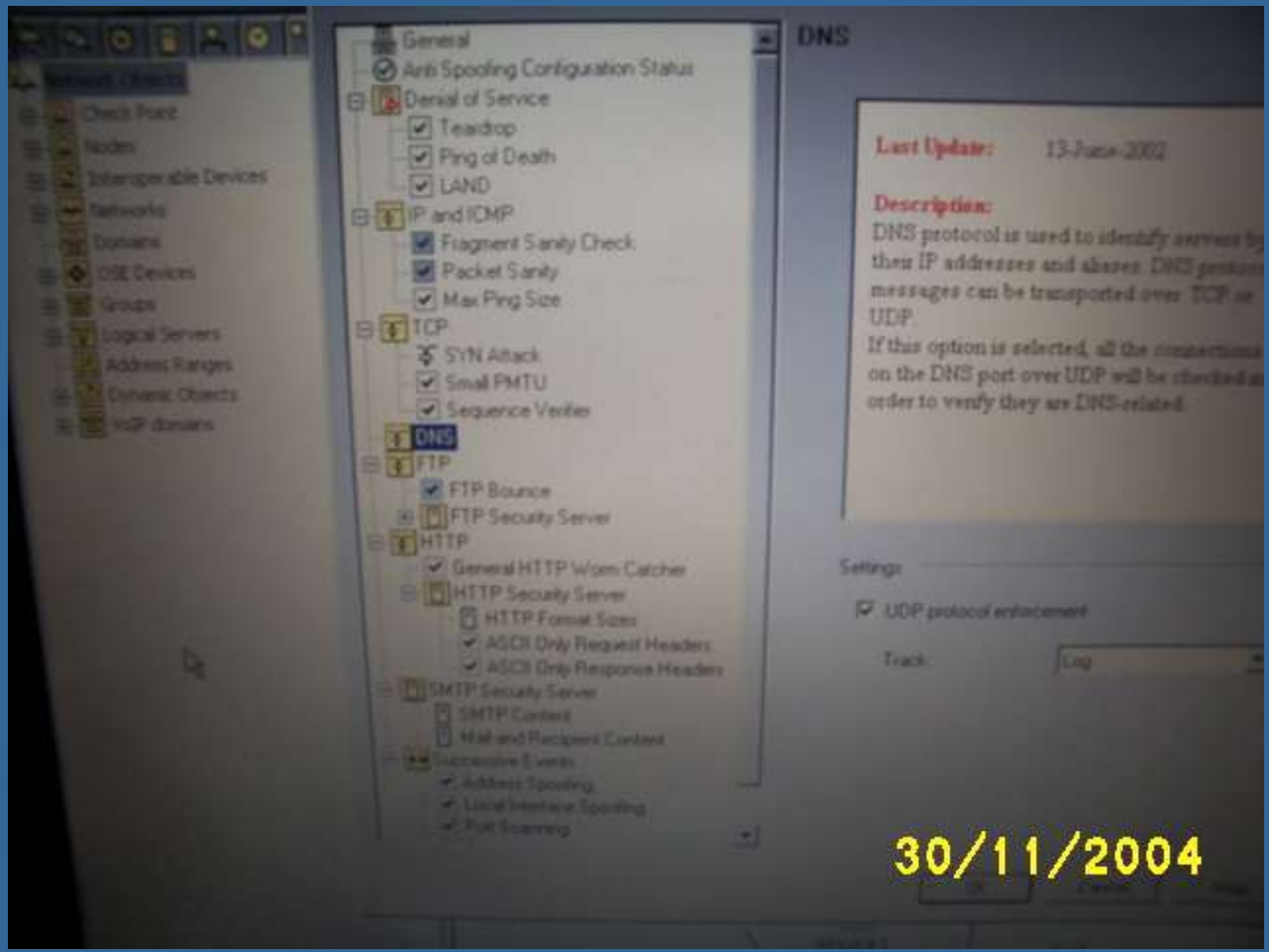
Checkpoint

Smart Defense HTTP Options



Checkpoint

Smart Defense Options

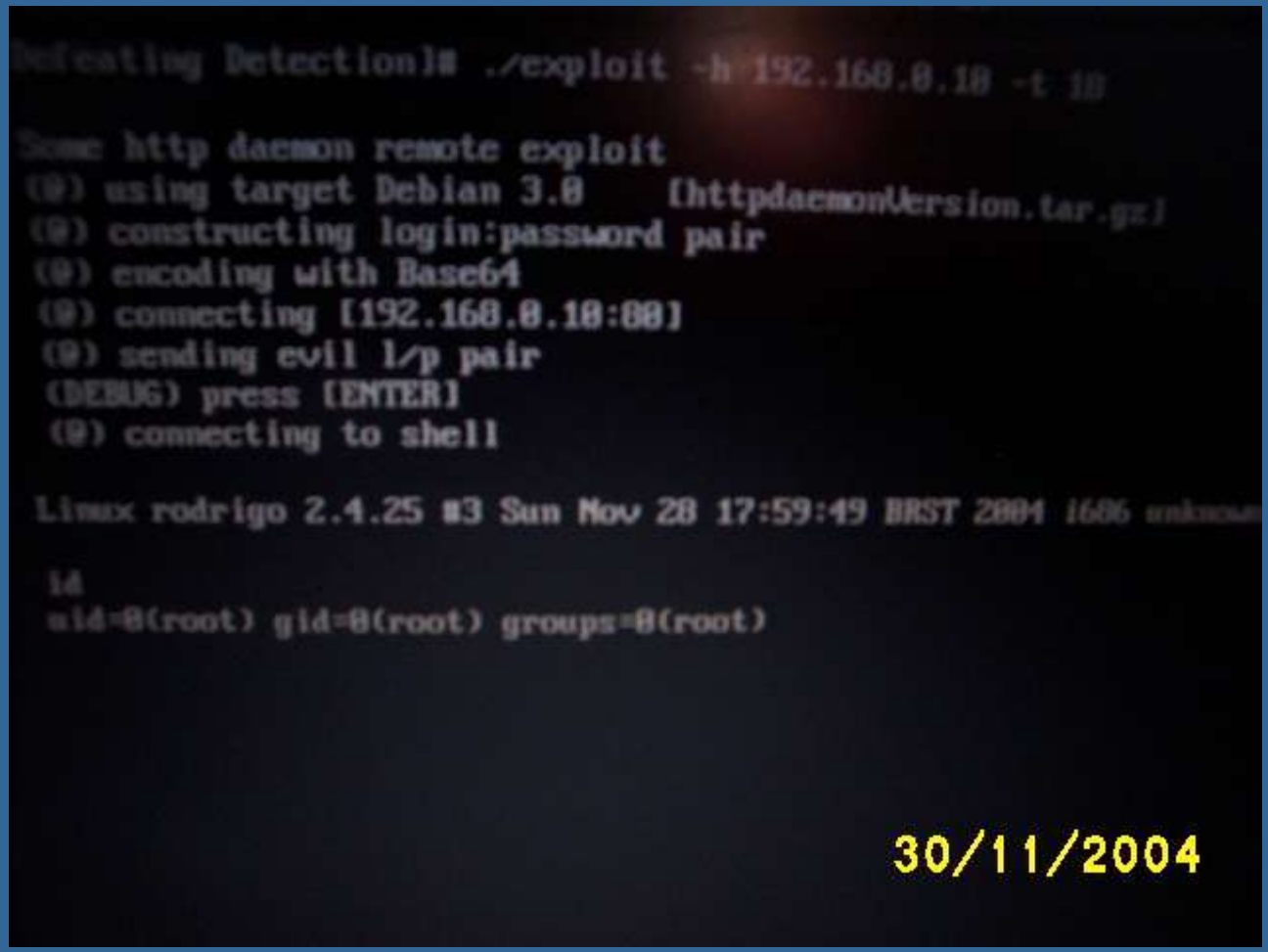


Vuln. Machine

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

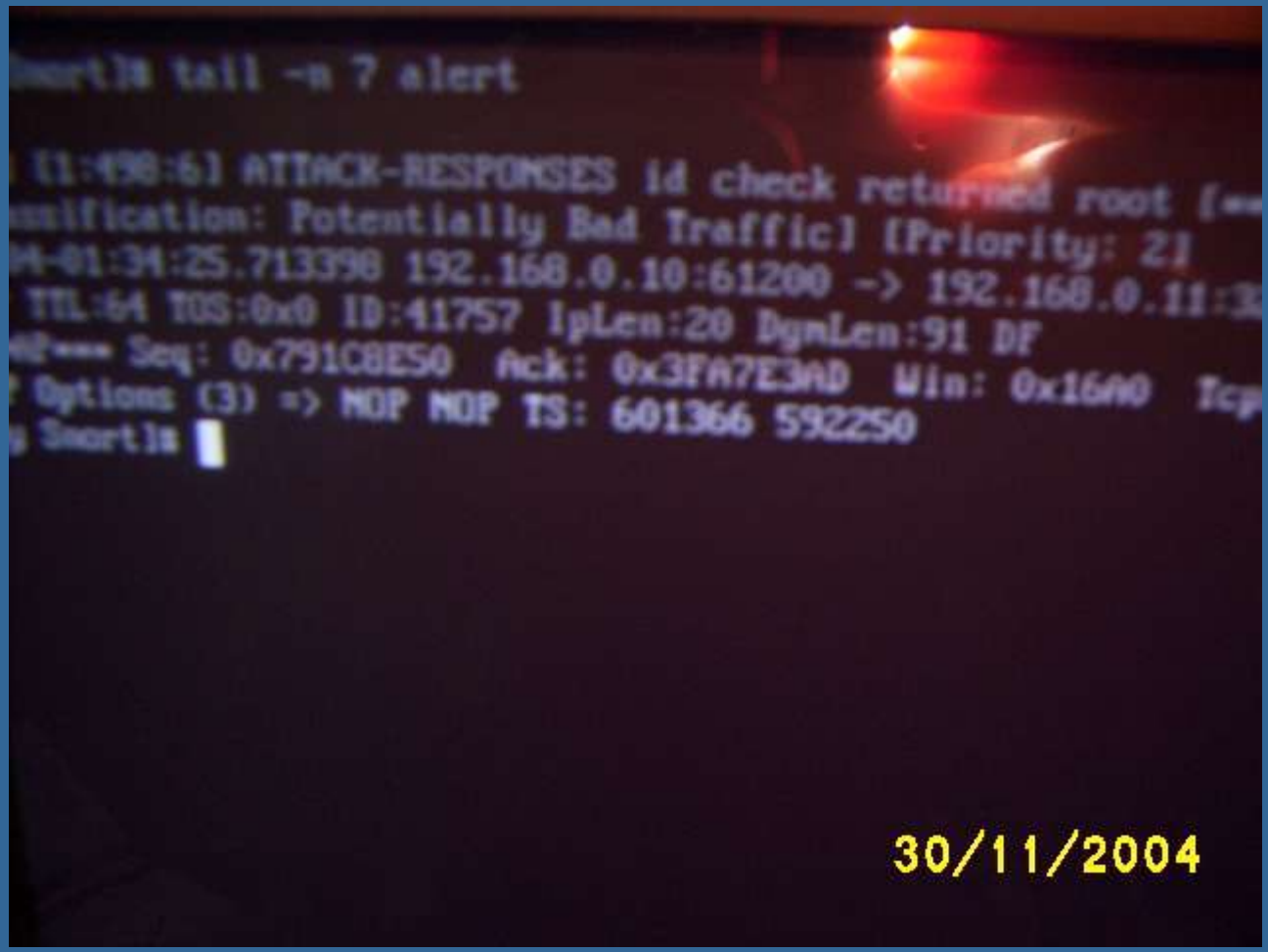
Launch the Attack!

Exploitation... as you can see, root!



IDS Results

Snort has detected the response of ID command

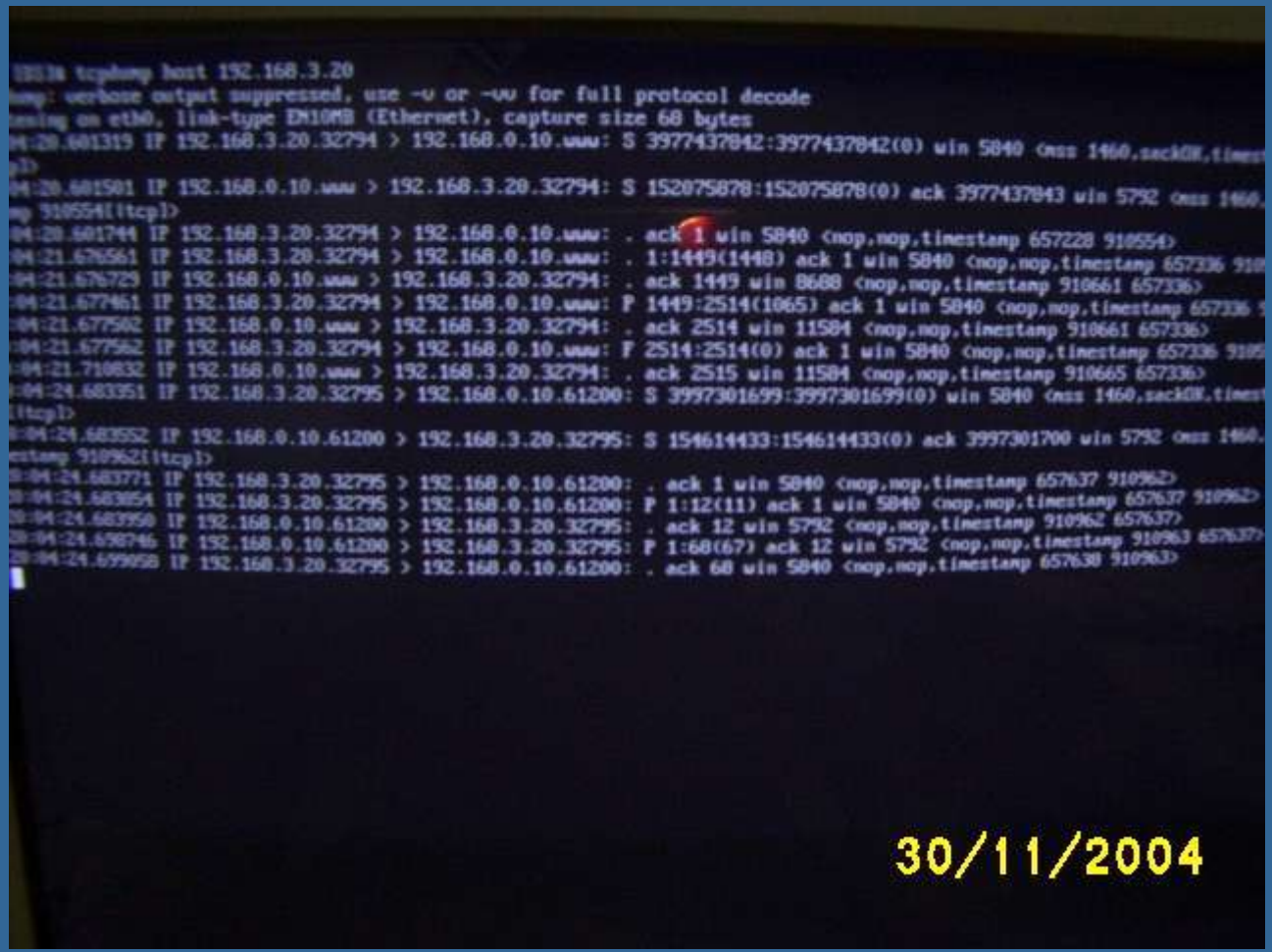


Attacking Again

Exploitation again, without ID command... checkpoint doesnt break (see) anything)

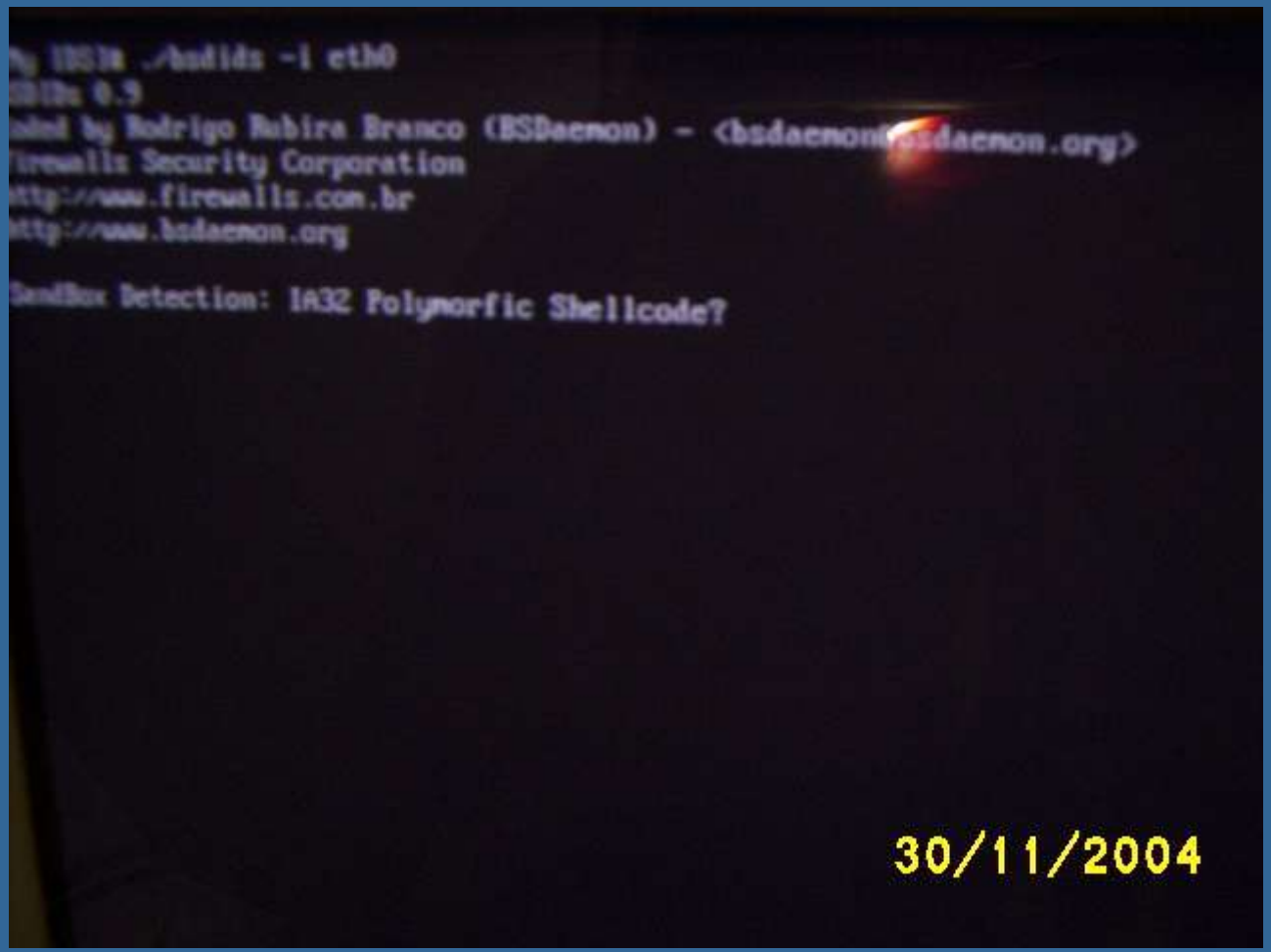
Sniffer Output

TCPDump Output of exploitation



DEMO IDS with Sandbox

My idiot IDS with “Sandbox” technology



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.

The END!

Doubts?!?

Rodrigo Rubira Branco
rodrigo@firewalls.com.br
bsdaemon@bsdaemon.org