Alexander Cannell

3/27/2013

CSIS 4700

Professor Rob Robertson

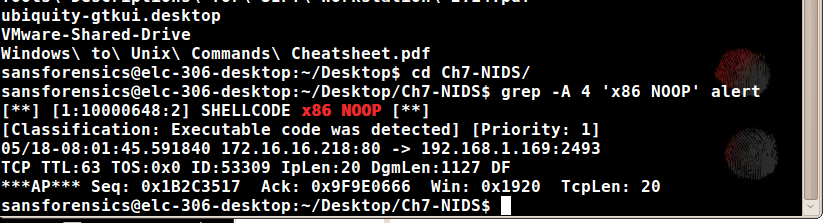
Chapter 7: Inter0ptic Saves the Planet

**Introduction:**

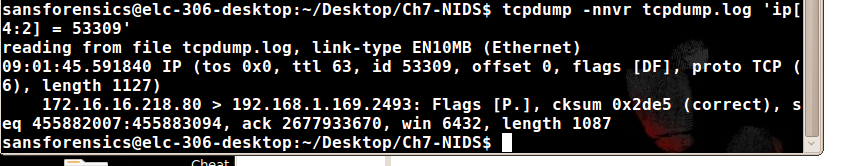
In his quest to save the planet, Inter0ptic has started a credit card number recycling program. “Do you have a database filled with credit card numbers just sitting there collecting dust? Put that data to good use!’ he writes on his web site. “Recycle your company’s used credit card numbers! Send us your database, and we’ll send you a check.” For good measure, Inter0ptic decides to add some bells and whistles to the site too MacDaddy Payment Processor has deployed Snort NIDS sensors to detect an array of anomalous events, both inbound and outbound. An alert was logged at 08:01:45 on 5/18/11 concerning an inbound chunk of executable code sent to port 80/tcp for inside host 192.168.1.169 from external host 172.16.16.218. The programs I use is tcpdump, snort, grep, and alert.

**Supporting Documentation:**

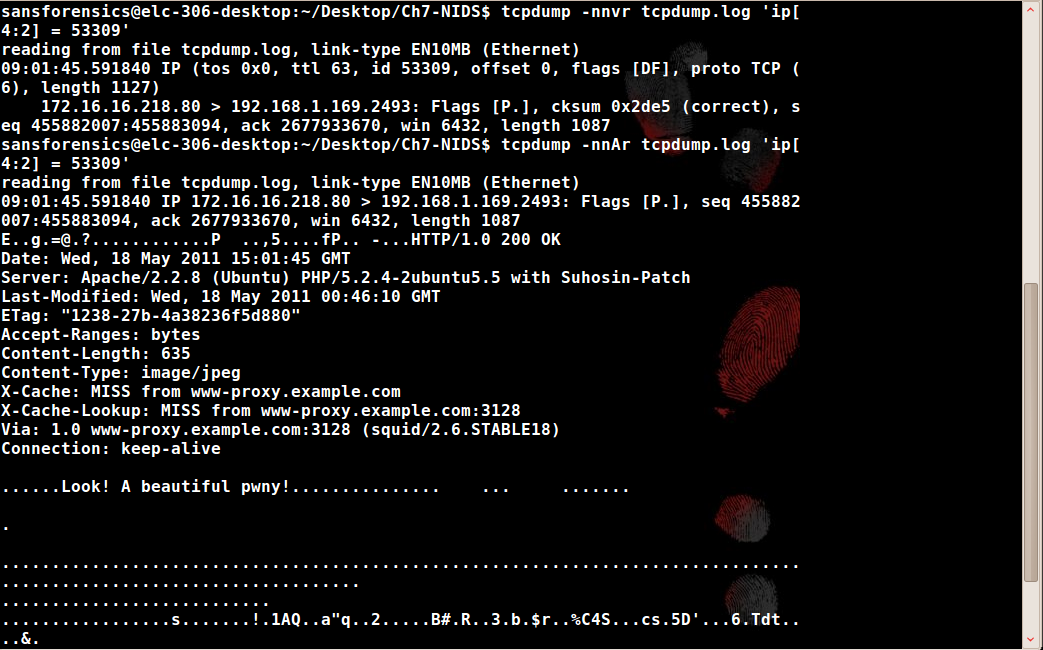
This is the alert that the security staff will initially provide.

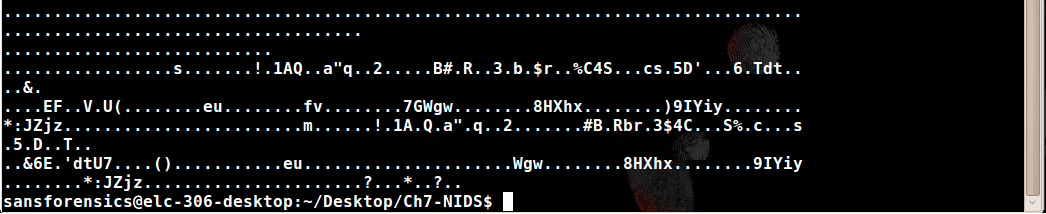


Using tcpdump to filter alert 53309.

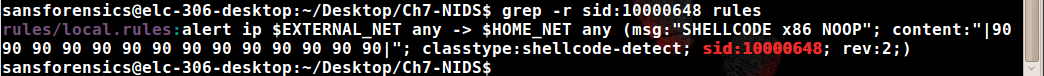


Examining the packets contents in ASCII.

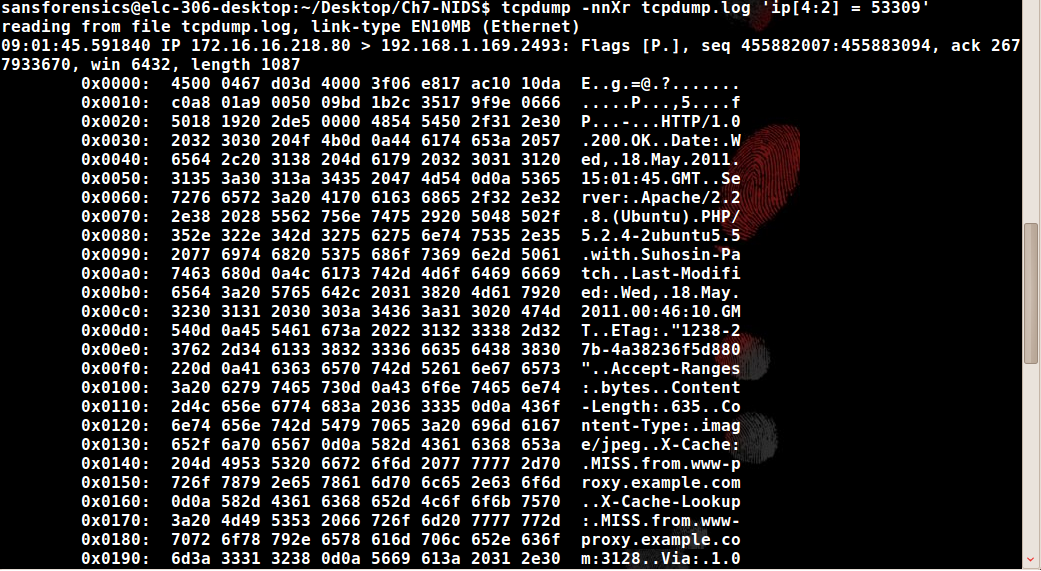


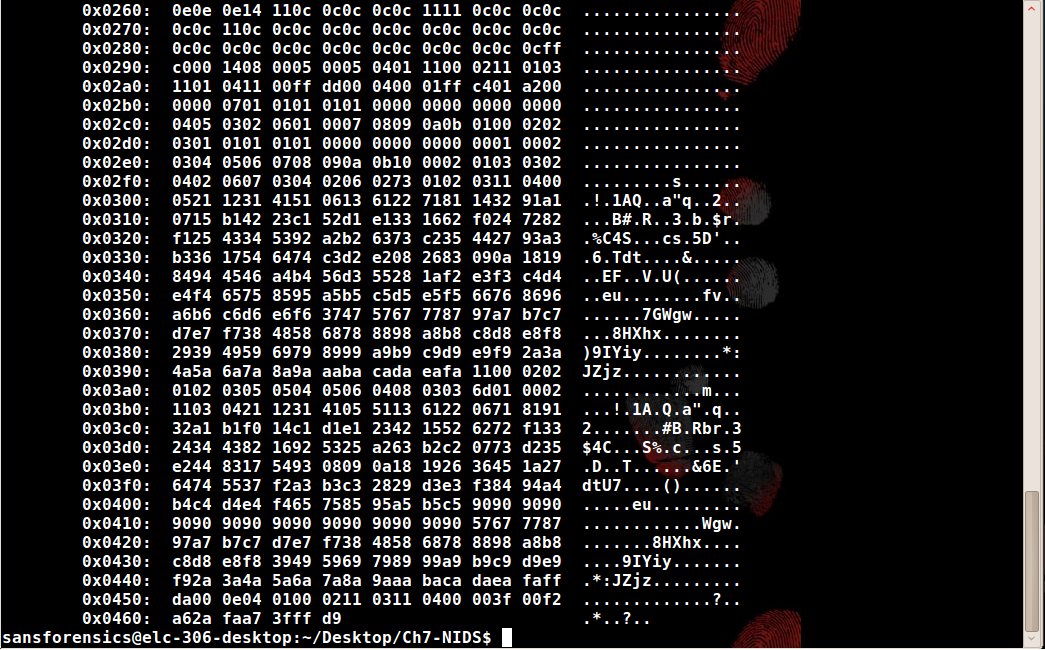


Using Snort to evaluate the rules.

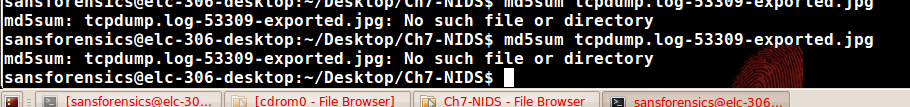


Using tcpdump to view the packets in both hex and ASCII.



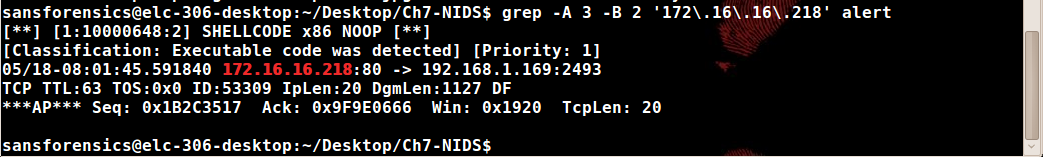


Im not getting anything with the command of md5sum tcpdump.log-53309-exported.jpg

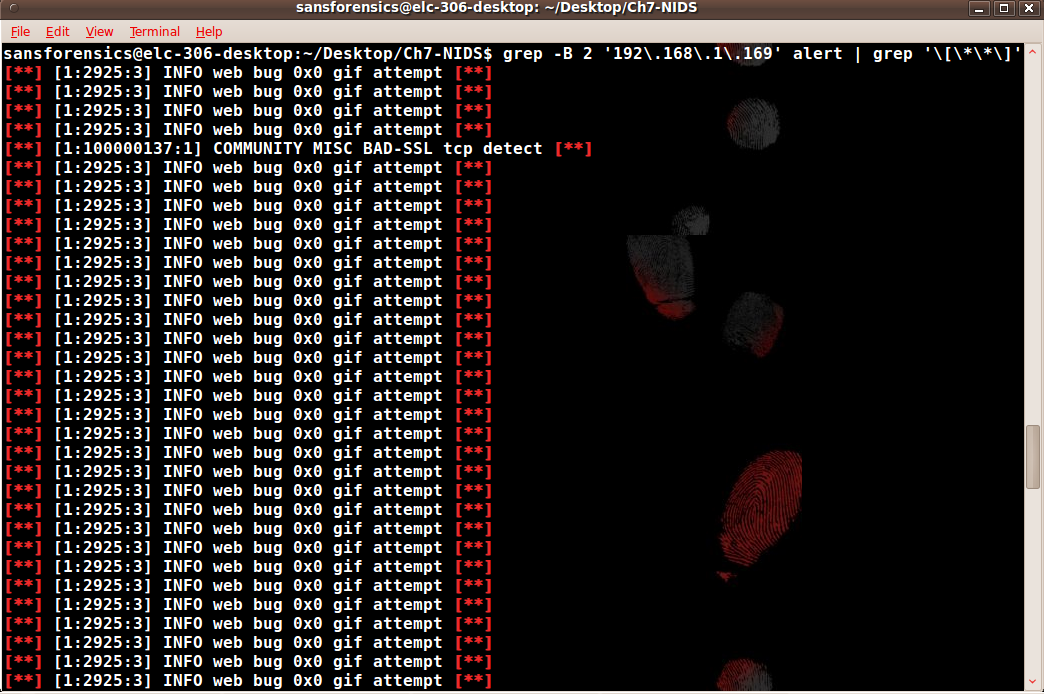


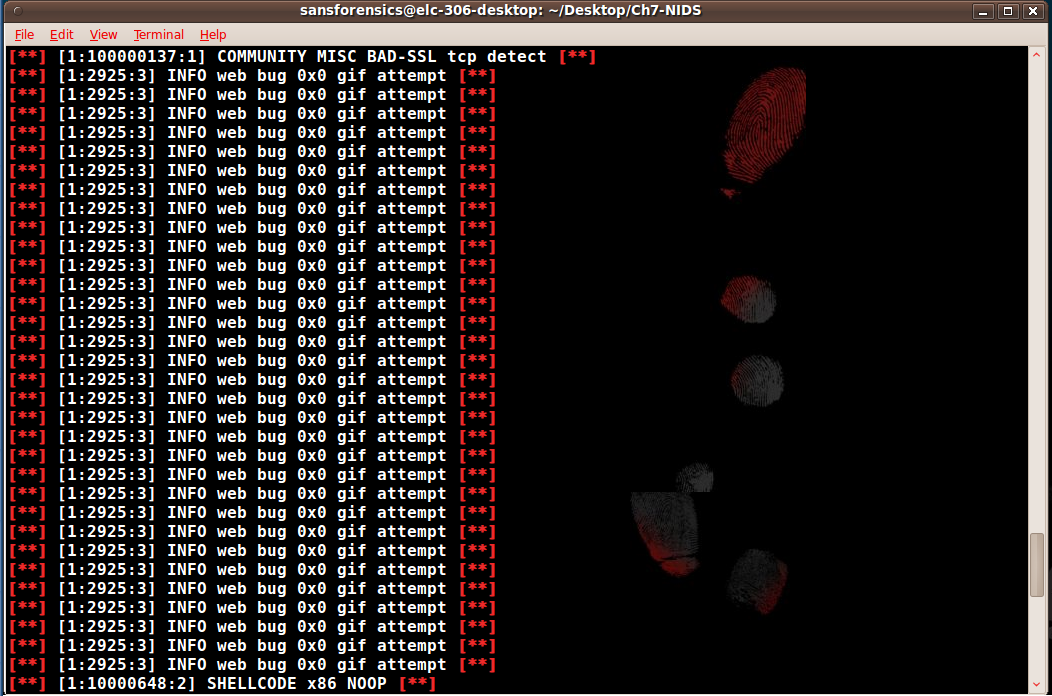
Im not getting anything with the command of sha256sum tcpdump.log-53309-exported.jpg

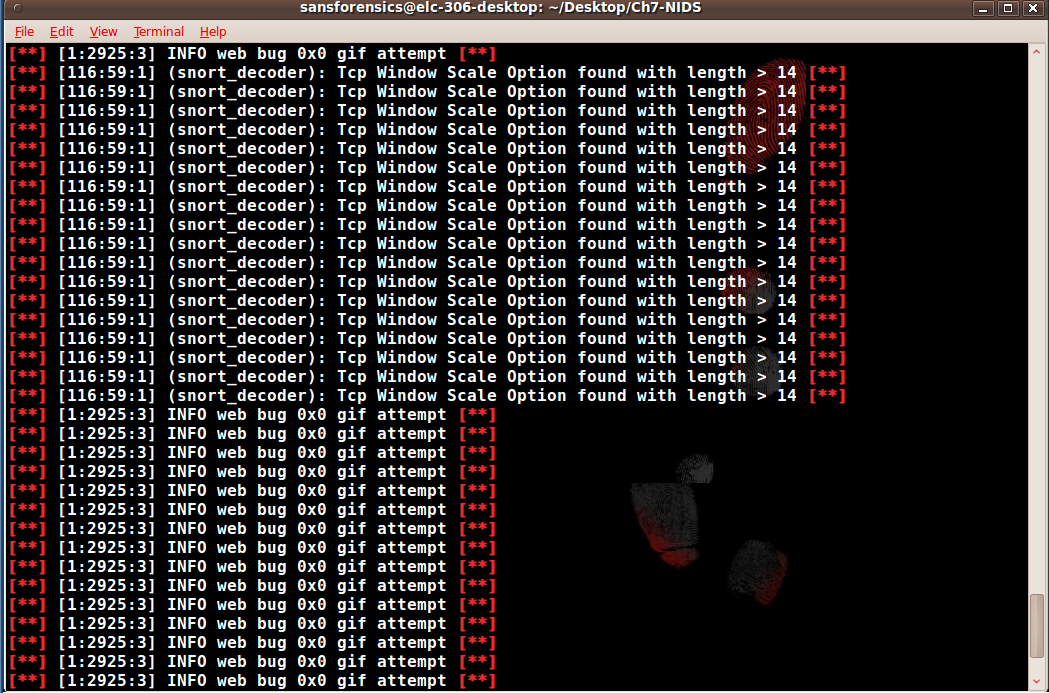


we can look at the behaviors of the systems.

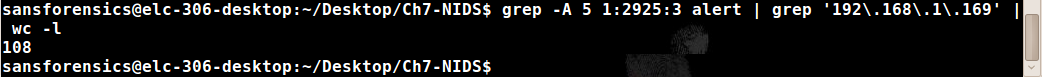
grep out all alerts relating to the target IP address 192.168.1.169.



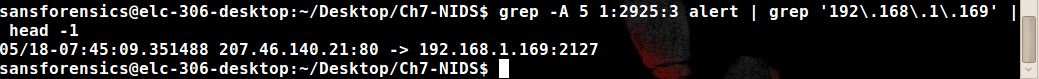




By using the wc –l command we can see how many events happened.



We can look at the start alert with head -l

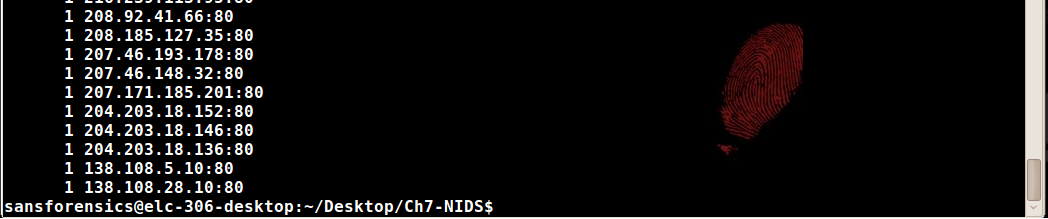


We can look at the end alert with tail -l

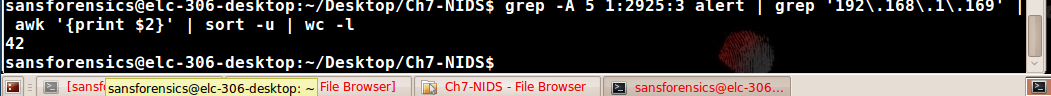


We can look at the web results from 07:45 to 08:15 on 05/18.

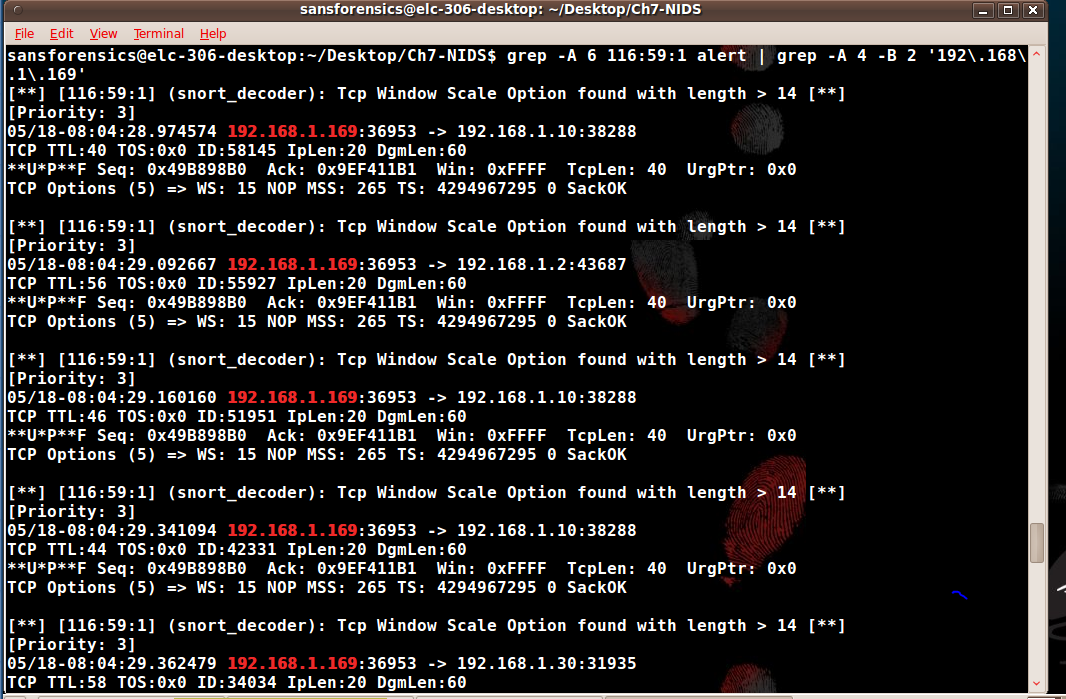


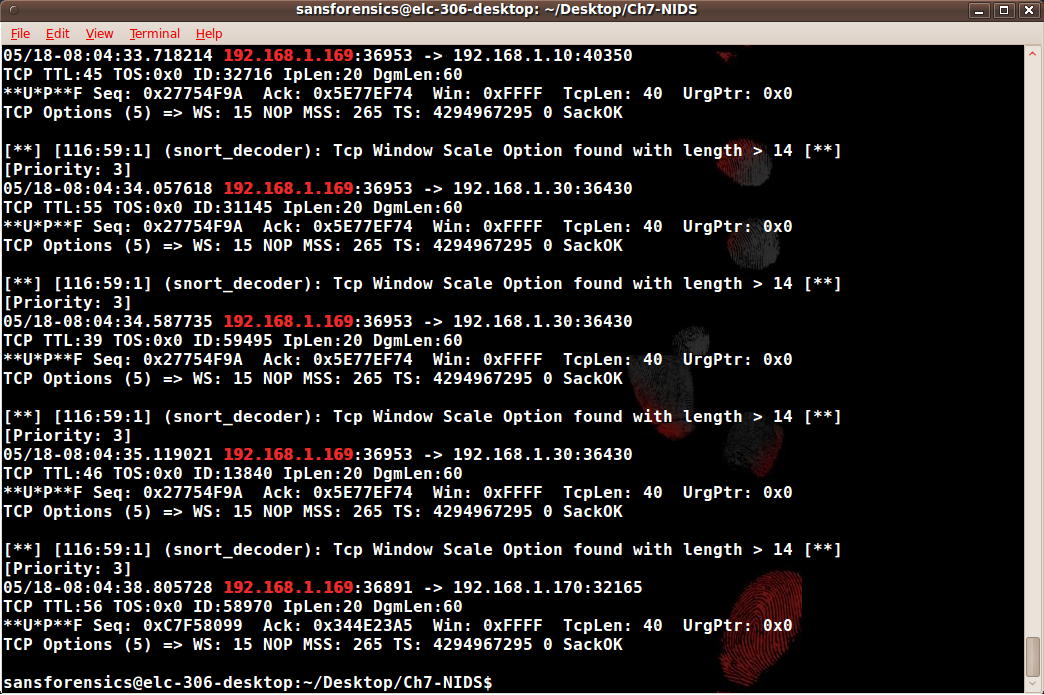


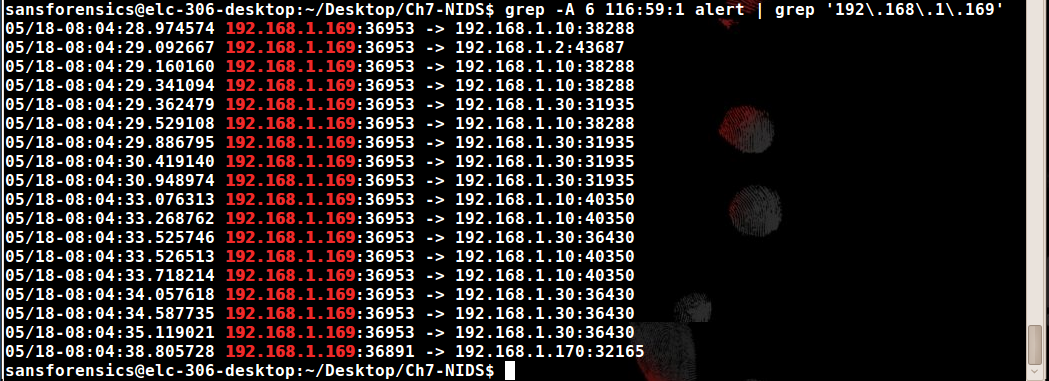
It appears that there are 108 alerts from 42 web servers.



TCP window Scale Option







**Examination:**

1. First, determine if the alert is true or false
   1. Examine the alert's data to understand the logistical context.
   2. Compare the alert to the rule, in order to better understand what it has been built to detect.
   3. Retrieve the packet that triggered the alert.
   4. Compare the rule to the packet to understand why it fired.
2. Subsequently, you will want to determine if there are any other activities that are related to the original event
   1. Construct a timeline of alerted activities involving the potentially malicious outside host.

From 07:45;09 to 08:15:08 on May 18th 2011, the address 192.168.1.169 browsed websites, some of which downloaded web bugs. At 08:01:45 the IP address 172.16.16.218 transferred a JPEG to 192.168.1.169, which had a weird binary sequence which was associated with buffer overflow exploits. The ETag on the web server was 1238-27b-4a38236f5d880. The hash of the JPEG was 13c303f746a0e8826b749fce56a5c126. At 08:04:28, 192.168.1.169 spent 10 second sending crafted packets to the other people on the network.

* 1. Construct a timeline of alerted activities involving the target.

The NIDS alerts for 192.168.1.169 start. The web bug starts to download at 07:45:09. They don’t show any adverse behavior, they do serve to establish a known commencement of web surfing. At 08:01:45 NIDS alerts for possible shellcode being downloaded by 192.168.1.169, this is the NIDS alert that alerted stimulus of our in investigation. Next we received 18 NIDS alerts of crafted packets sent from 192.168.1.169. The alerts end at 08:15:08.

Conclusion:

We can see that the host 192.168.1.169 computer surfs websites that introduces a web bug, that starts to download weird stuff with shell code. From 07:45;09 to 08:15:08 on May 18th 2011, the address 192.168.1.169 browsed websites, some of which downloaded web bugs. At 08:01:45 the IP address 172.16.16.218 transferred a JPEG to 192.168.1.169, which had a weird binary sequence which was associated with buffer overflow exploits. The ETag on the web server was 1238-27b-4a38236f5d880. The hash of the JPEG was 13c303f746a0e8826b749fce56a5c126. At 08:04:28, 192.168.1.169 spent 10 second sending crafted packets to the other people on the network. The NIDS alerts for 192.168.1.169 start. The web bug starts to download at 07:45:09. They don’t show any adverse behavior, they do serve to establish a known commencement of web surfing. At 08:01:45 NIDS alerts for possible shellcode being downloaded by 192.168.1.169, this is the NIDS alert that alerted stimulus of our in investigation. Next we received 18 NIDS alerts of crafted packets sent from 192.168.1.169. The alerts end at 08:15:08. It is suspected that it was a drive by exploit be couse of the Shellcode x86 NOOP. We can also see that we have tome subsequent reconnaissance which is an alert that there was something wrong on 192.168.1.0/24. The question we have to ask ourselves is why are the traffic patterns so consistent? The system must have been compromised, so we will have to perform the addiquit processions in the future.