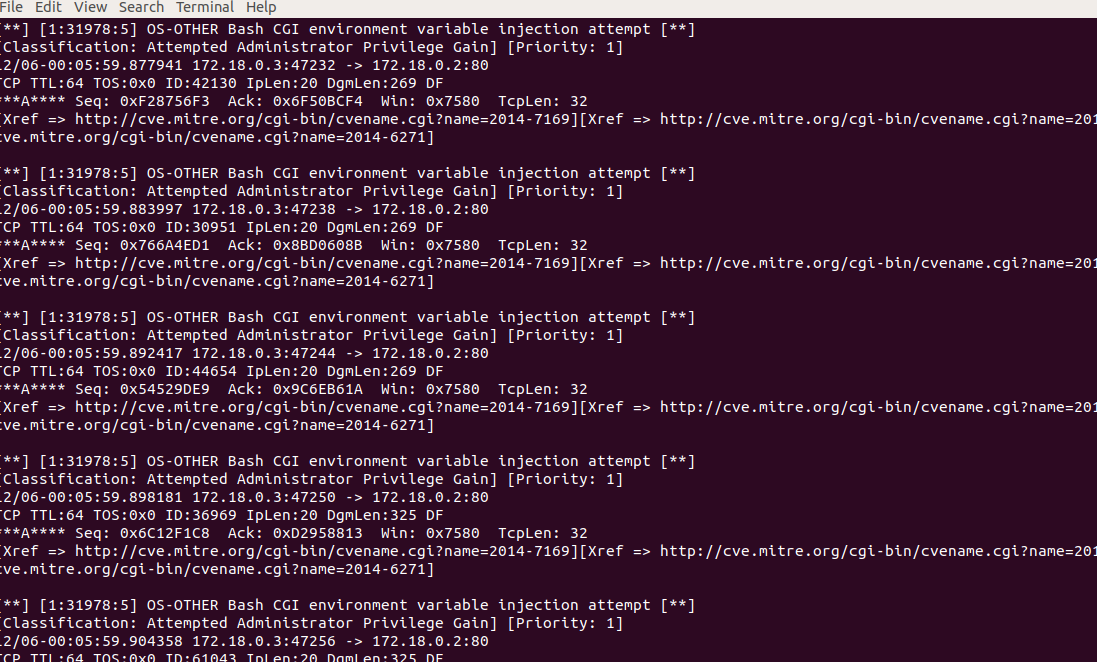
**Post-Incident Report**

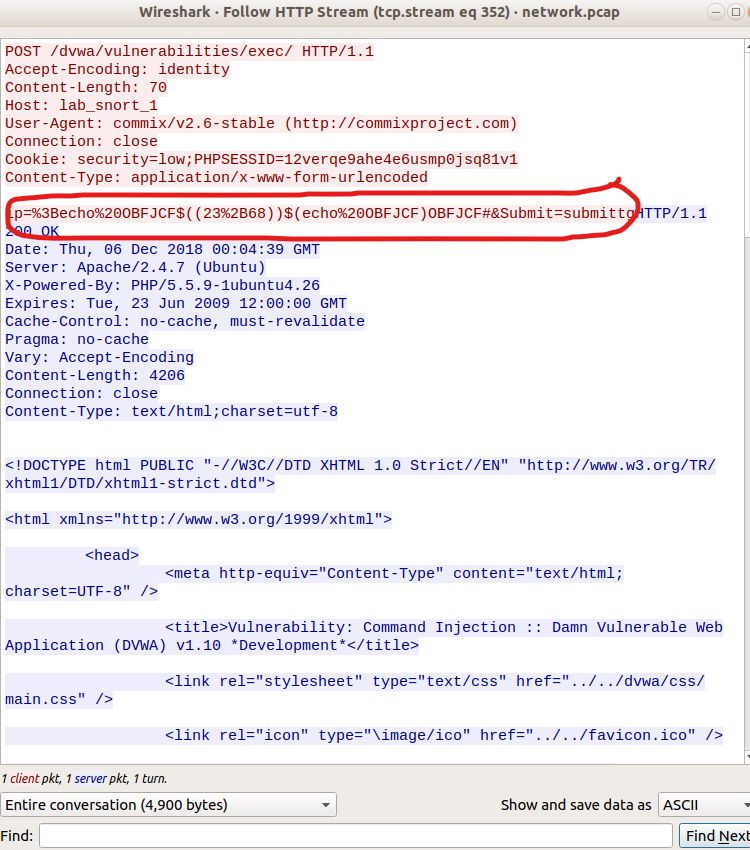
|  |  |
| --- | --- |
| Date of investigation | Nov 30th, 2019 |
| Date of incident | 2018-12-05 05:59 UTC |
| Outcome | True Positive - Bash CGI environment variable injection attempt |
| Action Taken | Identify the server that is being attacked and update to the most recent version of the Bash package by running the following command: Raw  # yum update bash |
| Reporting tool | Snort Alerts |
| Attack vector (Web, Email, Network, etc.) | This attack was propagated using a malicious Web Link, so it is a Web Attack |
| Source IP/email | 172.18.0.3 |
| Source port | 47232 |
| Destination IP/email | 172.18.0.2 |
| Destination port | 80 |

**Narrative**

• Alerted by Snort:



* Followed the tcp stream and located where there was an attempt to inject code into html page.



• Located Source/Destination IP Addresses and timestamp from Alerts:

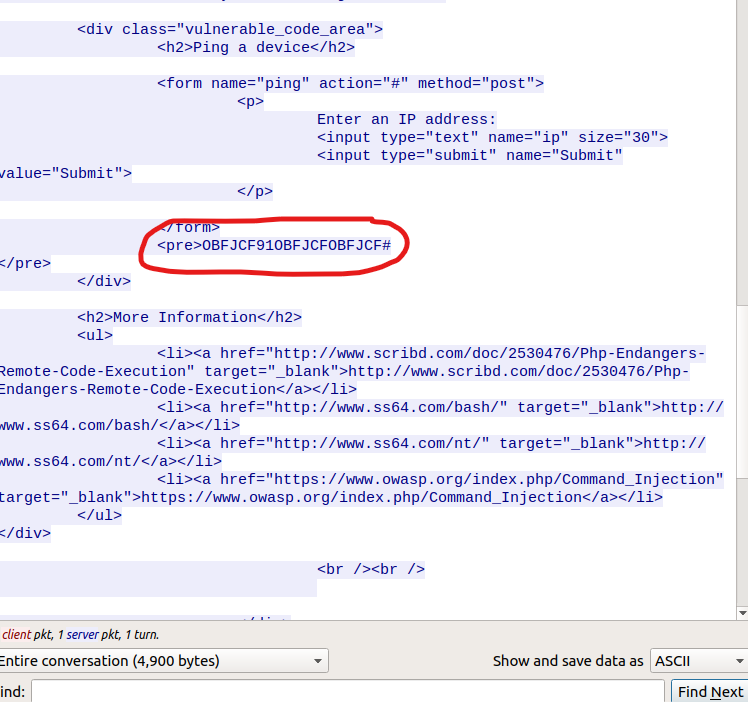
◦ Src/Prt: 172.18.0.3:47146

◦ Dst/Prt: 172.18.0.2: 80

◦ Time Stamp: 2018-12-05 19:04

**Post-Incident Report**

**Re**: Following the TCP Stream shows the client response to the code injection

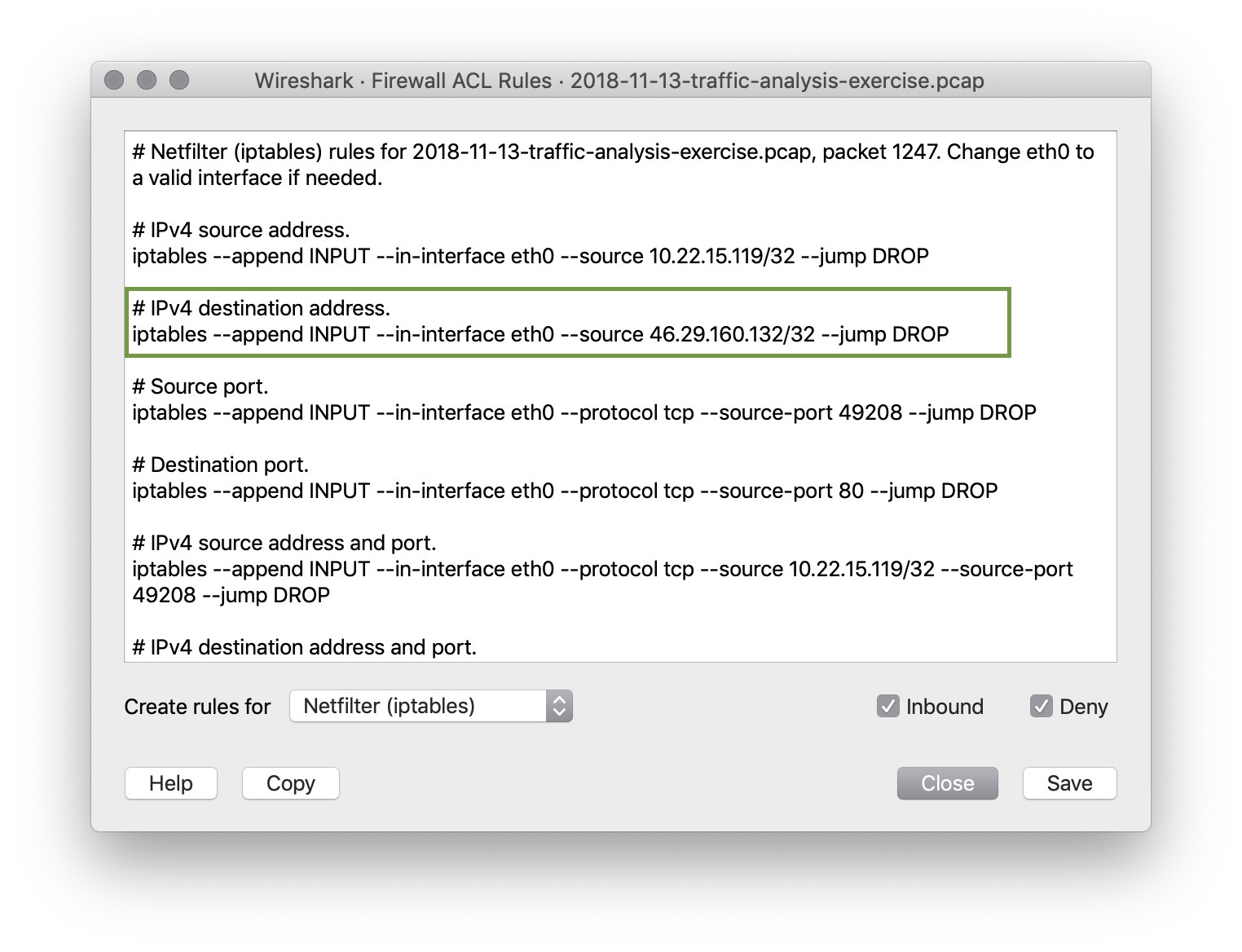


**Conclusion**: We have confirmed that there was an attempt to inject code into a website. Logs indicate that the attempt was no successful at gaining access.

**Re**: “Potential Corporate Privacy Violation”

• We can block malicious IP by using Wireshark and navigating to Tools > Firewall ACL Rules.

* #IPv4 Destination IP
* iptables --append INPUT --in-interface eth0 --source 46.29.160.132/32 --jump DROP



**Conclusion**: TRUE positive, this attack was propagated using a malicious Web Link, so it is a Web Attack