**DOE CDC Incident Report Template *powered by***

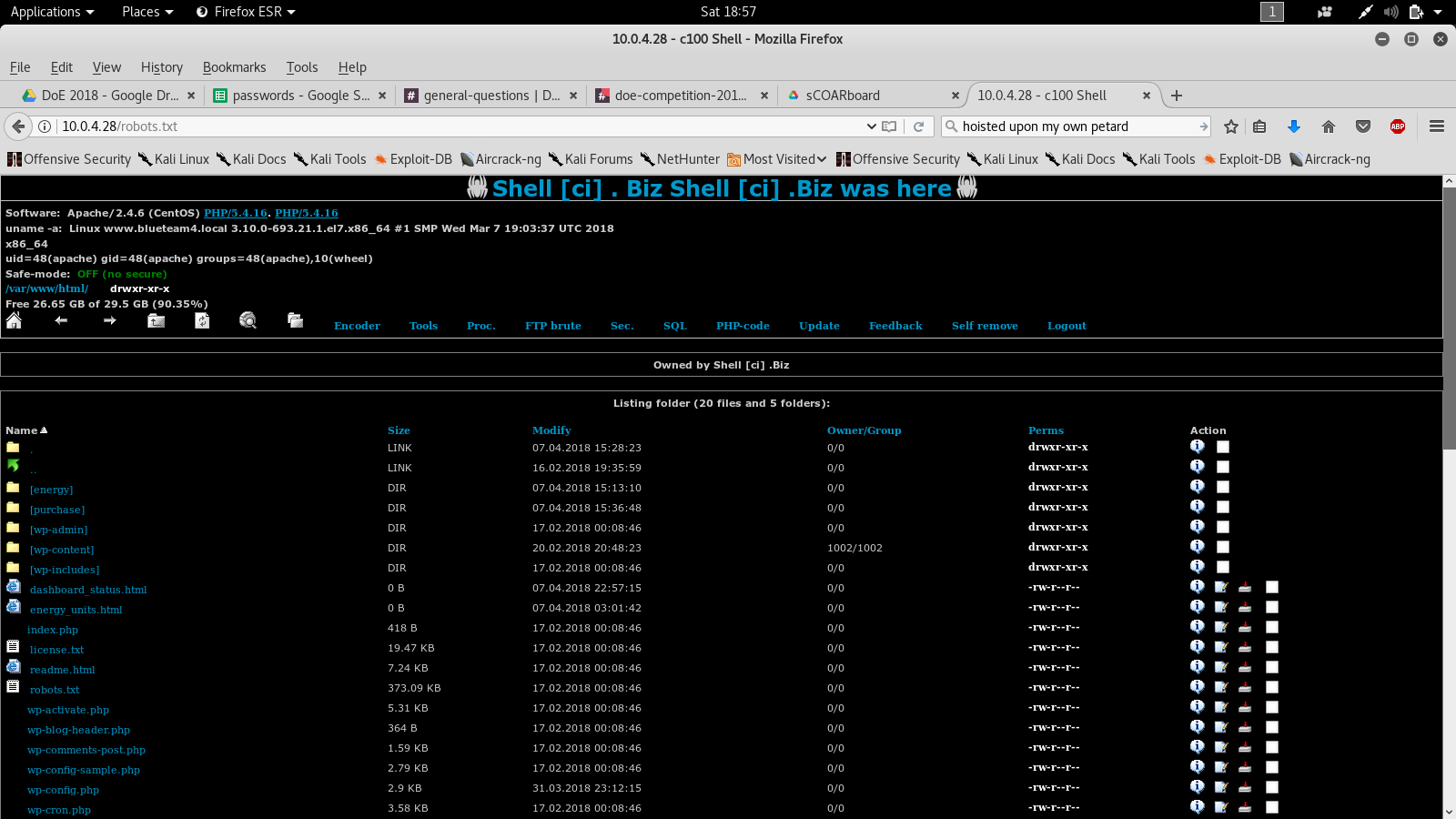
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REPORTED BY:** | Mike Petty |  | **DATE OF REPORT:** | 4/7/2018 |
| **TITLE / ROLE:** | Security |  | **INCIDENT NO.:** | 7 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INCIDENT ASSESSMENT:** | **NEGLIGIBLE:** |  | **MINOR:** |  | **SIGNIFICANT:** |  | **CRITICAL:** | **xx** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION** | | | | | | | | | | | | | |
| **DATE OF INCIDENT:** | | **4/7/2018** | | | | | | | |  | **TIME OF INCIDENT:** | | **6:30 PM** |
|  | **TITLE / ROLE:** | | | **Security** | | | |
| **PHONE:** | | **(704) 364-8886** | | | | | | | |  | **EMAIL:** | | **jcompto4@uncc.edu** |
| **LOCATION:** | | **OakRidge, TN** | | | | | | | | | | | |
| **SPECIFIC AREA OF LOCATION *(if applicable):*** | | | | |  | | | | | | | | |
| **INCIDENT TYPE:** | | | Remote code execution | | | | | | | | | | |
|  | | | | |  | | | | | | | | |
|  | | |  | | | | | | | | | | |
| **NO. OF HOSTS AFFECTED:** | | | 1 | | | |  | | **SOURCE IP ADDRESS:** | | |  | |
| **IP ADDRESS:** | | | 10.0.4.78 | | | |  | | **COMPUTER / HOST:** | | | centoswebserver | |
| **OPERATING SYSTEM:** | | | CentOS | | | |  | | **OTHER APPLICATIONS:** | | |  | |
|  | | | | | |  | | | | | | | | |
|  | | | | | |  | | | | | | | | |
| **INCIDENT DESCRIPTION:** | | | | | | | | | | | | | |
| Bad actors used a Remote Access Tool(RAT) located in robots.txt to gain access to the system and deny access to the administrators. | | | | | | | | | | | | | |
| **IMPACT ASSESSMENT:** | | | | | | | | | | | | | |
| Critical. Administrators were denied access. | | | | | | | | | | | | | |
| **RESULTING DAMAGE:** | | | | | | | | | | | | | |
| Bad actors locked administrators out of system. | | | | | | | | | | | | | |
| **IMMEDIATE ACTION TAKEN:** | | | | | | | | | | | | | |
| Administrators began analyzing logs in splunk to understand how the hackers continued to add users to the machine as well as how they were granted sudo access. We reverted to an older backup and moved the centos web server to a new IP so that the Red Team would stop attacking our web server while we got back into the box. | | | | | | | | | | | | | |
| **PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:** | | | | | | | | | | | | | |
| Administrators parsed through logs within splunk to find the web shell located in the robots.txt file then continued to use the string request the attackers used to create a new account and give it sudo permissions. After doing this the administrators were able to shutdown the web, server and continued to remove the robots.txt file from being hosted on the wordpress website. | | | | | | | | | | | | | |
| **ADDITIONAL INFORMATION:** | | | | | | | | | | | | | |
| “Hoisted upon my own petard.” | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION SHARING** | | | | | | | | |
| **DEPARTMENT REQUIRING NOTIFICATION** | | | **POINT OF CONTACT NAME** | | **DATE OF NOTIFICATION** | | | |
| CISO | | |  | | 4/7/2018 | | | |
| **REPORTING STAFF NAME:** | Jackson Compton | **REPORTING STAFF SIGNATURE:** | | Jackson Compton | | **DATE:** | 4/7/2018 |

**Report adapted from material located on SmartSheet.com**

****