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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REPORTED BY:** | Mike Petty |  | **DATE OF REPORT:** | 4/7/2018 2:23 PM |
| **TITLE / ROLE:** | Security |  | **INCIDENT NO.:** | 3 |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION** | | | | | | | | | | | | | |
| **DATE OF INCIDENT:** | | **4/7/2018** | | | | | | | |  | **TIME OF INCIDENT:** | | **2:23 PM** |
|  | **TITLE / ROLE:** | | | **Security** | | | |
| **PHONE:** | | **(704) 364-8886** | | | | | | | |  | **EMAIL:** | | **jcompto4@uncc.edu** |
| **LOCATION:** | | **Oak Ridge, TN** | | | | | | | | | | | |
| **SPECIFIC AREA OF LOCATION *(if applicable):*** | | | | | Oak Ridge National Labratories | | | | | | | | |
| **INCIDENT TYPE:** | | | Webpage scan | | | | | | | | | | |
|  | | | | |  | | | | | | | | |
|  | | |  | | | | | | | | | | |
| **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 actor using Nikto to scan website for vulnerabilities. | | | | | | | | | | | | | |
| **IMPACT ASSESSMENT:** | | | | | | | | | | | | | |
| None at the moment, it is a reconnaissance program that can be used to attack the website at a later date. | | | | | | | | | | | | | |
| **RESULTING DAMAGE:** | | | | | | | | | | | | | |
| None at the moment, but potentially dangerous in the future. | | | | | | | | | | | | | |
| **IMMEDIATE ACTION TAKEN:** | | | | | | | | | | | | | |
| Used modsecurity rule to ban the use of Nikto | | | | | | | | | | | | | |
| **PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:** | | | | | | | | | | | | | |
| Continue to monitor the webserver, to protect against future attack. | | | | | | | | | | | | | |
| **ADDITIONAL INFORMATION:** | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |

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

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REPORTED BY:** | Mike Petty |  | **DATE OF REPORT:** | 4/7/2018 2:23 PM |
| **TITLE / ROLE:** | Security |  | **INCIDENT NO.:** | 4 |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION** | | | | | | | | | | | | | |
| **DATE OF INCIDENT:** | | **4/7/2018** | | | | | | | |  | **TIME OF INCIDENT:** | | **2:23 PM** |
|  | **TITLE / ROLE:** | | | **Security** | | | |
| **PHONE:** | | **(704) 364-8886** | | | | | | | |  | **EMAIL:** | | **jcompto4@uncc.edu** |
| **LOCATION:** | | **Oak Ridge, TN** | | | | | | | | | | | |
| **SPECIFIC AREA OF LOCATION *(if applicable):*** | | | | | Oak Ridge National Labratories | | | | | | | | |
| **INCIDENT TYPE:** | | | Webshell | | | | | | | | | | |
|  | | | | |  | | | | | | | | |
|  | | |  | | | | | | | | | | |
| **NO. OF HOSTS AFFECTED:** | | | 1 | | | |  | | **SOURCE IP ADDRESS:** | | |  | |
| **IP ADDRESS:** | | | 10.0.4.78 | | | |  | | **COMPUTER / HOST:** | | | centoswebserver | |
| **OPERATING SYSTEM:** | | | CentOS | | | |  | | **OTHER APPLICATIONS:** | | |  | |
|  | | | | | |  | | | | | | | | |
|  | | | | | |  | | | | | | | | |
| **INCIDENT DESCRIPTION:** | | | | | | | | | | | | | |
| Webshell performed on system to gain unauthorized access to system. | | | | | | | | | | | | | |
| **IMPACT ASSESSMENT:** | | | | | | | | | | | | | |
| Critical, allowed bad actor onto the system, attempted to lock the administrators out of the system. | | | | | | | | | | | | | |
| **RESULTING DAMAGE:** | | | | | | | | | | | | | |
| None, connection was killed, bad actor blocked using custom script. | | | | | | | | | | | | | |
| **IMMEDIATE ACTION TAKEN:** | | | | | | | | | | | | | |
| Closed connections to protect system. | | | | | | | | | | | | | |
| **PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:** | | | | | | | | | | | | | |
| Continue to monitor the webserver, to protect against future attack. | | | | | | | | | | | | | |
| **ADDITIONAL INFORMATION:** | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |

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

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REPORTED BY:** | Mike Petty |  | **DATE OF REPORT:** | 4/7/2018 2:23 PM |
| **TITLE / ROLE:** | Security |  | **INCIDENT NO.:** | 4 |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION** | | | | | | | | | | | | | |
| **DATE OF INCIDENT:** | | **4/7/2018** | | | | | | | |  | **TIME OF INCIDENT:** | | **2:30 PM** |
|  | **TITLE / ROLE:** | | | **Security** | | | |
| **PHONE:** | | **(704) 364-8886** | | | | | | | |  | **EMAIL:** | | **jcompto4@uncc.edu** |
| **LOCATION:** | | **Oak Ridge, TN** | | | | | | | | | | | |
| **SPECIFIC AREA OF LOCATION *(if applicable):*** | | | | | Oak Ridge National Labratories | | | | | | | | |
| **INCIDENT TYPE:** | | | Directed Denial of Service | | | | | | | | | | |
|  | | | | |  | | | | | | | | |
|  | | |  | | | | | | | | | | |
| **NO. OF HOSTS AFFECTED:** | | | 1 | | | |  | | **SOURCE IP ADDRESS:** | | | many | |
| **IP ADDRESS:** | | | 10.0.4.78 | | | |  | | **COMPUTER / HOST:** | | | centoswebserver | |
| **OPERATING SYSTEM:** | | | CentOS | | | |  | | **OTHER APPLICATIONS:** | | |  | |
|  | | | | | |  | | | | | | | | |
|  | | | | | |  | | | | | | | | |
| **INCIDENT DESCRIPTION:** | | | | | | | | | | | | | |
| DDoS attack on webserver. 130 recurring connections at any one time, slowed down service to a crawl. | | | | | | | | | | | | | |
| **IMPACT ASSESSMENT:** | | | | | | | | | | | | | |
| Significant, slowed webserver down to rate at which executing commands on the system was near to impossible, and website would not load. | | | | | | | | | | | | | |
| **RESULTING DAMAGE:** | | | | | | | | | | | | | |
| Webserver and website held down by the DDoS. | | | | | | | | | | | | | |
| **IMMEDIATE ACTION TAKEN:** | | | | | | | | | | | | | |
| Used iptables to syncache. | | | | | | | | | | | | | |
| **PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:** | | | | | | | | | | | | | |
| Continue to monitor the webserver, to protect against future attack. Monitor splunk logs closely. | | | | | | | | | | | | | |
| **ADDITIONAL INFORMATION:** | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |

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

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