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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REPORTED BY:** | Mike Petty |  | **DATE OF REPORT:** | 4/7/2018 11:45AM |
| **TITLE / ROLE:** | Security |  | **INCIDENT NO.:** | 1 |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION** | | | | | | | | | | | | | |
| **DATE OF INCIDENT:** | | **4/7/2018** | | | | | | | |  | **TIME OF INCIDENT:** | | **11:45 am** |
|  | **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:** | | |  | | | | | | | | | | |
|  | | | | |  | | | | | | | | |
|  | | |  | | | | | | | | | | |
| **NO. OF HOSTS AFFECTED:** | | | 1 | | | |  | | **SOURCE IP ADDRESS:** | | | 10.0.250.163 | |
| **IP ADDRESS:** | | | 10.0.4.78 | | | |  | | **COMPUTER / HOST:** | | | centoswebserver | |
| **OPERATING SYSTEM:** | | | CentOS | | | |  | | **OTHER APPLICATIONS:** | | |  | |
|  | | | | | |  | | | | | | | | |
|  | | | | | |  | | | | | | | | |
| **INCIDENT DESCRIPTION:** | | | | | | | | | | | | | |
| Bad actor gained access to systemd/gopher, removed access to the administrators to access the system. Through examining logs, was able to determine was from nmap script. | | | | | | | | | | | | | |
| **IMPACT ASSESSMENT:** | | | | | | | | | | | | | |
| System compromised, needed to be reverted to previous good snapshot. | | | | | | | | | | | | | |
| **RESULTING DAMAGE:** | | | | | | | | | | | | | |
| Minimal, down time of 15 minutes during revert. | | | | | | | | | | | | | |
| **IMMEDIATE ACTION TAKEN:** | | | | | | | | | | | | | |
| Reverting system to snapshot | | | | | | | | | | | | | |
| **PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:** | | | | | | | | | | | | | |
| Reverted snapshot to repair damage. | | | | | | | | | | | | | |
| **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 11:45AM |
| **TITLE / ROLE:** | Security |  | **INCIDENT NO.:** | 1 |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INFORMATION SECURITY INCIDENT INFORMATION** | | | | | | | | | | | | | |
| **DATE OF INCIDENT:** | | **4/7/2018** | | | | | | | |  | **TIME OF INCIDENT:** | | **12:45 am** |
|  | **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:** | | |  | | | | | | | | | | |
|  | | | | |  | | | | | | | | |
|  | | |  | | | | | | | | | | |
| **NO. OF HOSTS AFFECTED:** | | | 1 | | | |  | | **SOURCE IP ADDRESS:** | | | 10.0.250.163 | |
| **IP ADDRESS:** | | | 10.0.4.78 | | | |  | | **COMPUTER / HOST:** | | | centoswebserver | |
| **OPERATING SYSTEM:** | | | CentOS | | | |  | | **OTHER APPLICATIONS:** | | |  | |
|  | | | | | |  | | | | | | | | |
|  | | | | | |  | | | | | | | | |
| **INCIDENT DESCRIPTION:** | | | | | | | | | | | | | |
| Bad actor gained access to systemd/gopher, removed access to the administrators to access the system, using nmaps script. | | | | | | | | | | | | | |
| **IMPACT ASSESSMENT:** | | | | | | | | | | | | | |
| System compromised, needed to be reverted to previous good snapshot. | | | | | | | | | | | | | |
| **RESULTING DAMAGE:** | | | | | | | | | | | | | |
| Minimal, down time of 15 minutes during revert. | | | | | | | | | | | | | |
| **IMMEDIATE ACTION TAKEN:** | | | | | | | | | | | | | |
| Reverting system to snapshot | | | | | | | | | | | | | |
| **PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:** | | | | | | | | | | | | | |
| Reverted snapshot to repair damage. Searched for active and inactive scripts to remove. | | | | | | | | | | | | | |
| **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**