**NECCDC 2021 – LINUX Systems**

**Pace University - BergCyberSec**

**[INITIAL TASKS]**

Things that can be done when disconnected from the internet. This will be done in conjunction with initial manual threat hunting.

**Threat Hunting**

*Delete pre-installed installed SEIMs and associated directories.*

Splunk: /opt/splunk and /opt/SplunkForwarder

Wazuh: /var/ossec

Elastic Stack: /usr/share/elasticsearch, /usr/share/kibana, /usr/share/filebeat,

Graylog: /usr/share/graylog-server

*Check crontab configurations for unexpected script triggering.*

/etc/crontab

/var/spool/cron/crontabs

*Check for any malicious aliases of commands in /etc and individual user home directories.*

/etc/bashrc or /etc/bash.bashrc

/home/<user>/.bashrc

**iptables Configuration**

Implement iptables-service and Disable firewalld. Need sudo privileges.

systemctl disable firewalld

yum(apt-get) install iptables-services

systemctl enable iptables

systemctl start iptables

service iptables save

Ensure iptables Rules Persist

nano /etc/sysconfig/iptables-config

IPTABLES\_SAVE\_ON\_STOP="yes"

IPTABLES\_SAVE\_ON\_RESTART="yes"

Save iptables Rules

sudo iptables-save

sudo service iptables save

View iptables Rules

sudo iptables -S

Flush All iptables Rules

sudo iptables -F

**BASH Command Logging**

The filename will be different depending on whether it is a RHEL or Debian based Linux distribution.

sudo nano /etc/bashrc *or* sudo nano /etc/bash.bashrc

Enter the following code as a single line entry at the bottom of the file.

PROMPT\_COMMAND='LAST\_COMMAND=$(history 1 | sed 's/-/\\-/') && logger -i -p local5.info -t bash "$USER $(tty): $LAST\_COMMAND"'

Reload .bashrc parameters to start command logging.

sudo . /etc/bashrc (RHEL) or sudo . /etc/bash.bashrc (Debian)

**[POST CONNECTION]**

Tasks that can be done once the network firewall reconnects to the internet.

**Wazuh Agent Installation Debian LINUX**

Installation for the Wazuh Agent on a Debian Base. Enter the proper ip address within ‘ ’

curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.0.3-1\_amd64.deb && sudo WAZUH\_MANAGER='wazuh\_server\_ip\_address' dpkg -i ./wazuh-agent.deb

**Wazuh Agent Installation RHEL LINUX**

Installation for the Wazuh Agent on a Red Hat Enterprise Linux Base. Enter the ip address of the wazuh server within the ‘ ‘

sudo WAZUH\_MANAGER='wazuh\_server\_ip\_address' yum install <https://packages.wazuh.com/4.x/yum/wazuh-agent-4.0.3-1.x86_64.rpm>

Start the wazuh agent service

sudo systemctl start wazuh-agent