<INSERT COMPANY LOGO HERE>

Compromised nix System

Live Data Gathering Checklist

* Run Live Collection script

Run the “nix\_Live\_Response.sh” script from an external USB drive connected to computer. This script will perform functions such as copying Logs to the external USB drive and collecting information such as date, time, logged in users, process tree, system uptime, etc.

OR

* Copy contents of “log” folders

Command: *cp /var/log/\*.log\**

Command: *cp –r /etc/cron\**

* Determine date on the system

Command: *date*

* Determine hostname of the system

Command: *hostname*

* Determine logged in users on the system

Command: *who*

* Determine running processes on the system

Command: *ps aux --forest*

* Determine process tree (and arguments)

Command: *pstree –ah*

* Determine mounted disks/items

Command: *mount*

* Review output of disk utility

Command: *diskutil*

* Determine loaded kernel extensions

Command: *kextstat –l*

* Determine system uptime

Command: *uptime*

* Determine system environment

Command: *uname -a*

* Determine (more detailed) system environment

Command: *prinenv*

* Determine OS kernel version

Command: *cat /proc/version*

* Determine running process memory usage

Command: *top –n 1 -b*

* Determine running services

Command: *service –status-all | grep +*

* Determine all loaded modules

Command: *lsmod | head*

* Determine last logins

Command: *last*

* Review contents of /etc/passwd

Command: *cat /etc/passwd*

* Review contents of /etc/group

Command: *cat /etc/group*

* Determine last login per user

Command: *lastlog*

* Determine “who” logged in user is

Command: *whoami*

* Determine “logname”

Command: *logname*

* Determine “id”

Command: *id*

* Review .bash\_history for each user

Command: *cat /home/<USERNAME>/.bash\_history*

* Determine current network connections

Command: *netstat -anp*

* Check for PROMISC adapters

Command: *ip link | grep PROMISC*

* Determine socket statistics

Command: *ss*

* Determine list of open files and network connections

Command: *lsof –i –n -P*

* Determine routing table

Command: *netstat -rn*

* Determine ARP table

Command: *arp -an*

* Determine network interface information

Command: *ifconfig -a*

* Review allowed hosts

Command: *cat /etc/hosts.allow*

* Review denied hosts

Command: *cat /etc/hosts.deny*

THEN

* Create image of disk

*Use FTK Imager to Acquire Disk Image*

EVIDENCE NUMBER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EXAMINER NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_