Security Incident Response Procedure

Overview

In the event of a computer security incident, the Computer Security Incident Response Team (CSIRT) will respond. If possible, two or more CSIRT members should be participating in a security incident. From the ticket opening to the ticket closing, a timeline and strict documentation should be kept, detailing events as necessary.

Goals

1. Detecting Sensitive Data Exposure
2. Detecting Vulnerability that Allowed Incident to Occur
3. Remediation and Prevention

Procedure

At any time, if a piece of equipment comes under custody of the CSIRT, a chain of custody form will need to be filled out and maintained.

Pre-Investigation

1. Create Incident Work Order
    1.1. Security Incident or CSIRT Incident
2. Obtain relevant system information
    2.1. IDS Logs, complaint/incident description, problem
    2.2. System Admin/Owner, System Location, MAC Address, IP Address, DNS Name
    2.3. If identifying system information cannot be obtained through IP Control or MESA, contact NOC to locate switch/port the system has been using. Trace system to room jack.
    2.4. If deemed necessary, disconnect the system from the network
3. Obtain information about system's function and sensitivity if possible
    3.1. If webserver, what web site does it serve? Etc.
4. If the system is known to be sensitive in nature or the machine is actively attacking other machines or there is evidence of criminal activity, immediately escalate to CSIRT status and contact the Exec. Dir. of ITSPMO, Deputy CIO, or the CIO. If necessary, call in police and proceed to step 8 of System Investigation when a forensic copy of the hard-drives in suspect machine have been obtained.

System Investigation

1. Interview with System Administrator, System Owner, and/or System User
    1.1. Classify system
    1.2. Identify system function
    1.3. Ask about recent activity, etc.
2. Obtain Administrator access on the suspect machine
    2.1. System Administrator can grant this

    2.2. If administrator access cannot be obtained through system administrator or owner, use of a password cracking tool can be used.
3. Run CSIRT Information Gathering Tool
    3.1. Obtain system information (Hardware, OS)
    3.2. Obtain networking information (# NICs, network addresses, etc.)
    3.3. Obtain logging information (System events, syslogs, etc.)
    3.4. Obtain account information
    3.5. Obtain services/program information
4. Run Sensitive Information Scan
    4.1. Scan for SSNs
    4.2. Scan for CCNs
5. If the system has not been deemed sensitive and is not attacking computers on the university's network, identify the problem and proceed to Problem Resolution.
6. Sensitive Information has been found - do the police need to be contacted?
    6.1. If so, contact Det. Tom Bacigalupi from Police Dept. STOP investigation. When possible obtain forensic copy of hard-drive from police and continue at step 8 if necessary.
7. Unplug system and bring to Security Lab
8. Create Forensic copy of hard-drives on system
9. Create Alterable copy of hard-drives on system
10. Run FTK to obtain file system information (files, content, etc.)
11. Mount alterable copy as read-only and investigate

Problem Resolution

1. Problem has been identified.
2. Recommend solution and talk with System Owner to determine who to work with for problem resolution.
3. If necessary, create separate report for system owner.
4. Close Work Order

Reporting

1. Prepare Final Report
    1.1. Include Timeline, Interview Q&A, Asset Inventory, People Involved, Sensitivity Finding, Problem, and Resolution