NCSA Cyber Threat Hunting Program

Document Name: NCSA Cyber Threat Hunting Program
Version: 0.9
Accountable: James Eyrich
Authors: James Eyrich and Adam Slagell

Reviewed: June 24, 2021
Approved: pending IIB approval

Purpose

In addition to the use of Qualysguard for vulnerability management of production systems, the NCSA Incident Response and Security Team performs active threat hunting on the entire NCSAnet to detect misconfigurations, system that are not compliant with University policies, and general system weaknesses. The goals of this program are (1) to detect issues more broadly for all networked assets and (2) to investigate more deeply than simple checklists for NCSA's most critical infrastructure.

Threat Hunting Activities

Automated scans by the NCSA Incident Response and Security Team allow detection of devices on every routable network to check for common problems and include:

- port scanning
- authentication attempts using common username/password combinations
- input validation testing (eg: web pages, APIs, logins)
- vulnerability identification

Manual investigations of critical infrastructure involve similar activities but also additional process logic testing and validation.

Responsibilities

We all have a shared responsibility to protect the systems and data we are responsible for and to follow NCSA and University policies and standards. Recognizing that hunting against systems may sometimes be disruptive, NCSA IRST takes extra precautions when hunting from privileged positions inside the NCSAnet (such as limiting scan rates and carefully monitoring for disruptions). Furthermore, NCSA IRST will inform system owners before any directed or manual penetration testing to help avoid tests during a critical operational window, though such testing will not generally perform any actions that a malicious threat on the Internet could not do at any time. And if one of the automated scans is causing disruptions IRST will work with service operator to mitigate the effects and prevent future problems.

It is also everyone's responsibility to report security incidents. If you believe your system is being attacked please follow NCSA Incident procedures, regardless if you think it might be a NCSA IRST system scanning or attacking. https://wiki.ncsa.illinois.edu/x/l5BgAQ Even if it turns out not to be a real attacker, it demonstrates organizational responsiveness.

Resolution

The security team is not the owner of risks, and sometimes neither is the system operator. When problems are identified that are not simple policy compliance, IRST will make recommendations for remediation. For simple issues this may just be a single ticket, and for more complex issues it may require meetings and a remediation plan from the service operator. Significant risks will also be raised to the Security Office when the attention of senior management is appropriate.