Operational Security & Lessons Learned from Recent Incidents/Vulnerabilities

Mine Altunay
OSG Security Team
Fermilab

Review of Operational Security Basics

- Incident Discovery and Reporting
  - If you suspect a security problem, please **report it immediately**.
  - First report to your **local/home organization's** incident response team.
  - Then report to OSG Security team:
    - Submit a "Security Incident" ticket at GOC (https://ticket.grid.iu.edu/goc/security).
    - Call the Grid Operations Center (GOC) at +1 317-278-9699.
    - Send email to security@opensciencegrid.org.
    - Everything is kept confidential

Review of Operational Security Basics

- Information needed in your report:
  - Your name; Email address; Phone number (easily reachable).
  - Your affiliation with the OSG. Virtual Organization, Site name?
  - Did this incident occur on a Site machine or on a VO machine or on your personal computer? Provide detailed information (names, IPs, URLs, etc.)
  - Do you think your grid identity (certificate and/or proxy) compromised?
  - A description of the incident, including time(s), systems and user accounts involved, and any related event ()
  - Any additional comments or questions you have

Review of Operational Security Basics

- What to Do After Reporting
  - **Do not turn the machine off**. There may be processes and/or live data that an incident responder may want to obtain
  - **Do not delete any files**. Do not wipe off and re-install the system.
  - **Get the machine off the network** so it cannot do any more damage. Unplug the network cable. If this is a remote machine, or you are not sure where the machine is, then contact the local security or networking group and have them block the machine at the border or at the network jack.

Lessons Learned from Incidents This Year

- 3 major incidents: 2 in EGI, 1 in OSG. All rooted and rootkits are installed.
  - EGI incidents, Incident 1
    - 5 separate AS/domains are compromised. Domain 1-- Attackers exploited a vulnerability in HP mgmt software. Exploit code was available for Windows domain only, but attacker adopted it into Linux.Collect ssh passwords.
    - Domain 0. Attacking node was also a grid node with a Oracle service with remote root vulnerability. 19 other nodes found to be compromised in this domain.
    - Domain 2. Attacked by Domain 0. 4 nodes are compromised. Exploited same HP vulnerability
    - Domain 3. attacked form Domain 2.

Lessons Learned from Incidents This Year

- Incident 2
  - Ssh attack, collecting passwords. Discovered because a cron job stopped working when Trojan ssh installed. Original incidents thought to happen 15 months ago. 10 systems, including a UI node.
- Incident 3:
  - SSHd was not patched up to date. Compromised and replace sshd. Contained in one site. Discovered when normal users could not log in

Lessons Learned from Incidents This Year

- Up-to-date patching is very important
- Once compromised, attackers collect ssh passwords and hop into other systems
- **We will demo a attack scenario in training session tonight**: port scan a grid node, break into ssh; we also demo what the sites can do to prevent and mitigate.
- Secure ssh installation. Will show in training session tonight

Best Security Practices & Lessons Learned

- **Keep your contact info up-to-date in OIM.**
- **Apply vendor and VDT patches.** OSG Security team will announce some of the important vendor patches, but it cannot cover everything
- **Do not run unnecessary services or open ports.** If you do not need ssh, turn it off. We talk about ssh in training session.
- **Do not trust all local users. Patch against local vulnerabilities.** Local users just as easily can get compromised and attackers can exploit local vulnerabilities

Best Security Practices & Lessons Learned

- **Configure ssh to prevent brute force attacks. Use a tool like Fail2Ban.** All incidents so far used ssh in some form. We will demo this evening how to apply Fail2Ban
- **Check executable permissions**
- **Send logs to a central server.** Helps a lot during mitigation and forensics.
- **Consider using TripWire or SamHain**. Helps during mitigation and forensics.

Best Security Practices & Lessons Learned

- **Once you discover a compromise: Use the guide we developed at**

(https://twiki.grid.iu.edu/bin/view/Documentation/BasicForensics)

  - Locate user processes
  - Find open files and ports
  - Find on which WN suspicious job run
  - Check md5 hashes of important binaries. Find out any rootkits are installed.
  - URL lists specific commands
  - Email local forensics team and/or OSG security team for help

Lessons Learned from Incidents This Year

- Discovering the compromise is hard. We will provide more help on this.
- **Our focus for the next year is to strengthen site security and do what sites cannot do for themselves**.