Cyber Security Topics

Tom Schlagel

Information Technology Division

April 10, 2009

BROOKHAVEN
NATIONAL LABORATORY

a passion for discovery

Office of Science
U.S. DEPARTMENT OF ENERGY

Agenda

- DOE-OIG Full Scope FISMA Audit
  - Phone number scans of the BNL site, including on-site housing
- Blocking of websites on the Visitor’s Wireless Network
- Conficker
- Questions?

DOE-OIG FISMA Full Scope Audit

- BNL is scheduled for a FISMA Full Scope Audit by the DOE Office of the Inspector General (DOE-OIG). KPMG carries out most of the auditing activities.
- Audit consists of:
  - External network vulnerability scanning and war-dialing
    - March 16 – April 3
  - Internal network vulnerability scanning
    - April 13 – 16
  - On-site visit auditing security controls, processes, procedures, with a primary focus on business systems (Finance, Procurement), but latitude to explore other areas
    - April 27 – May 15
- Findings from the audit are expected by June 30

DOE-OIG Full Scope FISMA Audit
External Network Vulnerability Testing

- All external IP addresses in BNL’s network address space are fair game.
- Auditor’s use a variety of tools to look for computers, services, applications to exploit. Particular focus on web applications with SQL injection vulnerabilities
- BNL had a few vulnerabilities of low risk that were fixed within a few days; generally looked very good
- KPMG’s IP addresses were whitelisted, otherwise BNL’s intrusion detection tools would have blocked them > 700 times

DOE-OIG Full Scope FISMA Audit
War Dialing

- Automatic dialing of all BNL extensions looking for answering modems to be used as a backdoor into the network
- The range of numbers was not split between work numbers and residence areas, so some of the housing areas received phone calls on March 19
- After getting user complaints, we contacted KPMG and they adjusted their dialing schedule

DOE-OIG Full Scope FISMA Audit
Internal Network Vulnerability Testing

- All internal IP addresses in BNL’s network address space are fair game, except for those that are whitelisted – this includes the networks being used for the RHIC Run, which are already protected by firewalls
- Same set of exploit tools used as for the external scanning.
- Scanning will begin on April 16 and last 4 days.

Block of websites

- Sporadic reports of websites that have been blocked that do not have objectionable content. These are the only types of websites that should be blocked at the proxies.
- May be related to SquidGuard application that runs on the proxies
- Extremely intermittent – happens infrequently, and is being investigated
- Recommendation is to fill out form that comes up when a site is blocked saying it is a mistake. This goes to Cyber Security to investigate, and they can correlate with events on the system.

Conficker at BNL

- Little activity as of April 1 (April Fool’s!)
- Payloads delivery began again April 9
- Still unknown exactly what the intent of Conficker is
- Lots of activity looking for signs of infections
  - Scanning – Nessus, US-CERT Tool
  - IDS signatures
  - So far, no infected systems at BNL
- *But if we detect an infected system on any BNL network, it will be immediately blocked*

Questions?