Security and Incident Response Process

Jim Barlow
<jbarlow@ncsa.uiuc.edu>
Head of Security Operations and Incident Response

National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign
Overview

- Targets
- NCSA's environment
- Incident Response Process
- Example incident
- Recommendations
Targets

- Everyone is a target for attacks
- Types of attacks one may see
  - Scans
  - Virus, worms, spam
  - Brute force
  - DDoS
  - Intrusions
  - Disgruntled employee
- Bottom line: Incidents are going to happen
Cybercrime survey

![Bar chart showing various types of cybercrimes and their percentages]

- Virus (including worms and trojans): 83.7%
- Spyware: 79.5%
- Port scans: 32.9%
- Sabotage of data or network: 22.7%
- Pornography (adult): 22.4%
- Laptop/Desktop/PDA theft: 15.5%
- Insider abuse of computer (pirated software/music): 15.0%
- DoS (Denial of Service): 14.5%
- Network intrusion: 14.2%
- Financial fraud: 13.4%
- None (skip to 18): 8.4%
- Telecom fraud: 5.3%
- Wireless network misuse: 2.9%
- Website defacement: 2.7%
- Pornography (child): 2.6%
NCSA's environment

- 360 employees
- 6000+ users
- 5000+ hosts
- Variety of platforms
  - Windows desktops to high end computing machines
- Most hosts on public IP space
- No firewall (for most machines)
Incident Response Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Education
Preparation

• Defense in depth
  • Network to host to user
• Have procedures in place
  • Security policies
• Designate people
  • NCSA has 4 security engineers on Incident Response team (can involve others if needed)
• Outside contacts
  • Other institutions
  • Law enforcement
Passive Security Measures

- Intrusion detection system (IDS)
  - Bro (network)
  - Samhain/Tripwire (host)
- Network flows
  - Cisco and Argus
- Centralized logging server
  - SEC and swatch
Active Security Measures

- Border blocks
- Host based firewalls
  - IPtables, XP SP2 firewall
- Firewall in main employee building
  - Netscreen
- Remote vulnerability scans
  - Nessus – Virtual Scanning Cluster (VSC)
Identification

- Through one of your own monitoring methods (IDS, flows, etc.)
  - Email or pager alerts
- Internal employee discovers problem
- Remote site
  - Email or 24x7x365 helpdesk
- Level of incident response depends on initial assessment of investigation
  - Virus, intrusion, harassment
- Is this time critical?
Containment

• Isolate problem
• Determine extent of damage
  • internal/external
• Start damage control process
  • Shutting down services
  • Quarantine hosts
  • Isolate network segments
• Is your network designed to do any of these easily?
Eradication and Recovery

- Collect evidence
  - Internal use, or for law enforcement?
  - Managing information
    - Incident tracking database (RTIR)
- Analysis
  - What fully happened and to what extent?
- Again, action may depend on severity of case
  - Collect for chain of custody, or wipe and reinstall?
- Backups, backups, backups
Education - Lessons learned

- Create an incident report
  - Internal and external
- Evaluate overall incident response process
- Ways to improve detection and prevention methods
  - Iterate back into monitoring and alerting
Example incident

- Identification
  - Network flow alert
  - Pulled network flows
  - Scanned machine
    - Backdoor detected
  - Scan rest of network for same port
    - Found two more hosts
Example incident, cont.

- Containment
  - Disabled network jacks or blocked at border
  - Determine what accounts and/or vulnerabilities used to gain access
    - Disabled account
- Eradication
  - Hands on analysis of some machines
  - Other hosts pulled and replaced
    - Saved original disks
- Recovery
  - Reinstall of machines
Example incident, cont.

- Lessons learned
  - Added signatures in monitoring systems
  - Shared external report with other TG sites
    - Similar incidents reported at other sites
- Had repeated attacks
- Time to call law enforcement
  - Notified U of I legal counsel
- Start process of working with FBI
- Stuck with case till end
- You never know where one alert will lead
Recommendations

- Preparation
- Get to know your area law enforcement agents
- Participate in organizations involved in IR
  - FIRST (www.first.org)
  - Infragard (www.infragard.net)
  - HTcia (www.htcia.org)
- Get involved in similar communities
  - ISAC (Information Sharing and Analysis Centers)
Questions?

Email: jbarlow@ncsa.uiuc.edu
http://www.ncsa.uiuc.edu/~jbarlow