Incident Response and Handling

Maryland Security Day
March 2, 2005

Cathy Hubbs, IT Security Coordinator
George Mason University
chubbs@gmu.edu
http://security.gmu.edu

Mason's CSIRT

- Fall 2004 began discussions to create CSIRT
- Exec & Tech members appointed
- Techs sent to SANS: Incident Handling training early December
- Fall plan called to formalize CSIRT process and communicate to University spring 2005

Mason's IT

- Central IT organization, ITU
- Departmental Systems Administrators
- SALT- Systems Administrator Leadership Team
- SALT listserv
- Server inventory
- ITU Risk Assessment

Mason’s Incident

- Discovered through routine log analysis
- Login attempts on 3 servers coming from same IP address
- IP address is internal-tracked to owner
- Part-time sysadmin reached on mobile
- Permission received to take server off line

CSIRT Process

- Preparation
- Identification
- Containment (Preserving Evidence)
- Eradication
- Recovery
- Lessons Learned

Preparation

What we did

- Enlisted CSIRT members
- Techs attended training
- Decided to use SANS forms to document
- Discussed using our reporting software-Magic

To do

- Prepare and maintain Jumpkit
- Customize forms
- Use tracking software for reporting and event correlation-Magic
- Communication plan
- Establish and widely distribute phone tree
- IDS/IPS
- Centralized syslogs

Mason's Jump Kit

- Contact information (pagers and cell phone numbers)
- Incident forms
- Backup devices & cables
- Blank Media: CD-Rs, DVD-Rs, usb-keys, floppies
- Laptop
- Composition notebook
- Utility CD: basic tools and built in commands, forensics software, port lists, security patches, packet sniffers and protocol analyzers

Mason's Utility CD

- Gathering evidence from the scene of an incident
  - Examining media
  - Examining system
- Investigating the evidence
- Analyzing evidence
  - Checking identities
- Supportive tools for handling evidences
- Recovering the system after an incident

Utility CD-Examining the media

These programs can be used to collect information about the state of systems or media either during an incident or afterwards.

- DD – data dump **Platform:** Unix (Built-in command)
  Can be used to make binary copies of computer media. Can be used as a simple disk imaging tool if given a raw disk device as its input.

- The Coroner's Toolkit (TCT) **Platform:** Unix
  A collection of programs that can be used for a post-mortem analysis of a Unix system after a break-in.

- Encase **Platform:** Windows
  Encase is a commercial evidence gathering and analysis tool, which performs all stages from imaging disks through investigation to preparing a final report.

Utility CD
Examining the system and processes

- Netcat **Platform:** Unix, Windows
  Used to create network connections, TCP or UDP, to or from any port number.

- sockstat **Platform:** FreeBSD (built-in command)
  Lists open sockets on a system. Can be used to identify any unexpected connections, for example from packet sniffers.

- Fstat **Platform:** FreeBSD (built-in command)
  Lists open files on a system. Can be used to identify any unexpected logfiles, for example from packet sniffers.

- Dumpreg - Dump Windows Registry **Platform:** Windows
  Free tool to dump the Windows Registry in text format for further processing.

Utility CD
Examining the system and processes

- Dumpevt - Dump Windows Event log **Platform:** Windows
  Free tool to dump the Windows Event log in text format for further processing.

- Foundstone Forensic tools **Platform:** Windows
  Toolkit includes programs to list open ports and the processes controlling them; to track logins and activity on Windows systems; to examine file access times and permissions.

- Sysinternals tools **Platform:** Windows
  Includes utilities to examine Windows processes, files and ports.

Utility CD
Checking Identities

- nslookup **Platform:** Unix, Windows (built-in command)
  Used to request information from the Domain Name Service. This can be used to look up names and IP addresses, can also help in diagnosing problems with the DNS or attempts to corrupt information within name server caches.

- Whois **Platform:** All
  Whois is a protocol commonly used to search databases for contact details.

- InterNIC **Platform:** All
  Provides a searchable Whois database which can be queried to trace the ownership of IP address ranges. The database has access to information about most of the generic top level domains, such as .com, .edu etc.

- traceroute **Platform:** Unix, Windows (tracert)
  Utility that traces the route that an IP packet follows to another internet host and prints the route.

Utility CD
Handling evidence

- Find **Platform:** Unix, Windows
  Can be used to search through a directory tree looking for files that have particular names, permissions, or almost any other combination of attributes..

- ps **Platform:** Unix
  Gives only a snapshot of the current processes, but no repetitive update.

- ls **Platform:** Unix (built-in command)
  List files and directories on a filesystem. It can be used to check for files that may have been installed by intruders during the course of an incident.

- Ifconfig **Platform:** Unix (built-in command)
  The ifconfig command is used to report the state of network interfaces on unix systems.

Identification: Signs of an Incident

- Unusual services on the system
- Unusual files on the system
- Disk space starts filling up
- System crashes or experience weird problems
- Data missing
- Spikes in network traffic or system utilization
- Calls to the Help Desk
- System event logs show probing or scanning or…

Identification

What we did

- Determined inside server-contacted owner/administrator
- Identified scope of incident
- Determined extent of damage
- Noted workstation and server dependencies
- Review services and processes

To do

- Preserve potential evidence by using non-invasive tools –Utility CD
- Contact NET
- Run network and port scans
- Is computer compromised?
  - IF yes
  - THEN stop and image
  - ELSE continue looking for artifacts

Containment

What we did

- Disconnected from network
- Checked task manager- looking for suspicious processes/services
- Directory searches
- Imaged the compromised systems.
- Examined system logs.
- Workstation dependencies.

To do

- Call NET scan network and ports
- Collect NET log files
- Disconnect the affected systems. Depends on incident, i.e., DOS
- Examine all system logs.

Eradicate → Recovery

- If in doubt about whether you found and removed everything?

Nuke from high orbit.

–Marcus Sachs SANS instructor

That is to say, rebuild.
Preferably from CD or original media.

Recovery

What we did

- Located new unused server
- Helped rebuild server
- Helped lock down server
- Took on administration of server
- Performed security assessments on additional servers.

To do

- Communicate policies
- Offer training
- Partner with outside sources

Incident Handling Lessons Learned

What we did

- Didn’t let our hair get on fire.
- Took notes-referred to forms and checklists.
- Got permission from data owner before taking charge.
- Telephoned CSIRT-Exec & Tech leads

To do

- Jump kit ready with plan to review software for updates at least quarterly
- Contact NET group first-prior to taking off network
- Perform network & port scans
- Use less invasive tools during investigation (i.e., no directory searches)
- Organize LL sessions as quickly as possible especially for techies.
- Ongoing CSIRT & first responder training.
- Use Magic-track all security incidents.

Next steps

Technical

- Risk Assessment- lock down targeted systems
- IPS/IDS
- Centralized logging
- Protect & Serve

People

- Communicate existence of CSIRT
- Provide technical training for CSIRT-techs and other potential first responders

Policies

- Data Stewardship + procedures
- Server Registration Policy

There are lots of possibilities on how the hack might have occurred

- Using NetBIOS vulnerability from internal users, enumerating users accounts and cracking passwords on the compromised server.
- Using SQL connections from the internet, port 1433 was open to the internet.
- Trojan running-allowing external connections.

Resources

- NIST Special Publication 800-61
  - Computer Security Incident Handling Guide-January 2004 http://csrc.nist.gov/publications/nistpubs/
- SANS S.C.O.R.E. http://www.sans.org/score
  - Incident Handling forms
  - Intrusion Discovery Cheat Sheets
- CHIHT - Clearing House for Incident Handling Tools
  http://chiht.dfn-cert.de/
- Carnegie Mellons CERT Coordinator Center
  - CSIRT Development Guides http://www.cert.org/csirts/
- Checking Microsoft Windows Systems for signs of Compromise http://www.ucl.ac.uk/cert/win_intrusion.pdf
- FIRST http://www.first.org/
  - Forum of Incident Response and Security Teams