Incident Response

1. What is an Incident?
2. Phases of Incident Response
   1. Preparation
   2. Identification
   3. Containment
   4. Damage Assessment
   5. Preserve Evidence
   6. Eradication
   7. Recovery
   8. Follow-up

What is an Incident?

Violation of security policy
- Unauthorized access of information
- Unauthorized access to machines
- Embezzlement
- Virus or worm attack
- Denial of service attacks
- Email spam or harassment
Detecting an Incident

- Catching perpetrator in the act
  - Unauthorized logins, NIDS alerts
- Noticing unauthorized changes in the system
- Receiving a message from another site, saying that your site was used to launch an attack on them
- Strange activities on system
  - Crashes, random reboots, slow performance

Incident Response

- Restoring system to satisfy site security policy
- Phases:
  1. Preparation for attack (before attack detected)
  2. Identification of attack
  3. Containment of attack (confinement)
  4. Damage assessment
  5. Preserve evidence (if necessary)
  6. Eradication of attack (stop attack)
  7. Recovery from attack (restore system to secure state)
  8. Follow-up to attack (analysis and other actions)

Preparation

- Configure intrusion detection systems
- Determine your response goals
- Document incident response procedures
  - Who to contact?
  - What to do?
- Organizing a CSIRT
  - Finding and training personnel
  - Hardware/software necessary for investigation
Incident Response Goals

1. Determine whether a security breach occurred
2. Contain the intrusion to prevent further damage
3. Recover systems and data
4. Prevent future intrusions of same kind
5. Investigate and/or prosecute intrusion
6. Prevent public knowledge of incident

Identification

- Who/what reported incident
- Date and time of the incident
- Nature of the intrusion
  - What level of unauthorized access was attained?
  - Is it known to the public?
- Hardware/software involved
  - How critical are the affected systems?
- Assemble CSIRT
  - Team membership may vary based on nature of incident

Containment

- Limit access of attacker to system resources
- Containment method depends on criticality of systems and extent of intrusion
  - Monitoring intruder
  - Reducing intruder's access
  - Deception
  - De-activating the affected account
    - Need to kill active processes too
  - Blocking access to system via firewall
  - Pulling network/phone cable
  - Powering down system
Monitoring

- Records attacker’s actions; does not interfere with attack
  - Idea is to find out what the attacker is after and/or methods the attacker is using
- Problem: attacked system is vulnerable throughout
  - Attacker can also attack other systems
- Example: type of operating system can be derived from settings of TCP and IP packets of incoming connections
  - Analyst draws conclusions about source of attack

Reducing Access

- Reduce protection domain of attacker
- Problem: if defenders do not know what attacker is after, reduced protection domain may contain what the attacker is after
  - Stoll created document that attacker downloaded
  - Download took several hours, during which the phone call was traced to Germany

Deception

Honeypot: system designed for intruders to attack, to waste their time and to allow safe monitoring
- ex: The Honeynet Project, honeyd

Deception Tool Kit
- Creates false network interface
- Can present any network configuration to attackers
- When probed, can return wide range of vulnerabilities
- Attacker wastes time attacking non-existent systems while analyst collects and analyzes attacks to determine goals and abilities of attacker

Experiments show deception is effective response to keep attackers from targeting real systems
Honeynet Project

- ool development
  - Environment simulation: virtual machines
  - Data control: firewalling tools to limit attacker activities to avoid damaging other systems
  - Data collection: network and keystroke loggers
  - Data analysis: tools to extract relevant data from tcpdump logs and more

Research and documentation
- Analysis of attacker and honeypot techniques
- Analysis of particular attacks

Damage Assessment: Data

- System date and time when assessment began
- List of users currently logged in
- Time/date stamps for filesystem
- List of processes
- List of open network sockets
  - Associated applications
  - Associated systems
- System configuration files
- Log and accounting files
- System date and time when assessment complete

Data Assessment: Procedure

Use trusted binaries from floppy/CDROM
- Use a trusted shell
- Set PATH to only use floppy/CDROM tools

System date and time:
> date
Mon Apr 26 13:33:08 EDT 2004

List of current users
> w
1:33pm up 30 day(s), 3:34, 3 users, load avg:0.26
User tty login@ idle JCPU PCPU what
root console 9:21am 4:13 -sh
wald pts/14 15Apr04 3:25 66:24 63:06 -bash
root pts/20 9:21am 4:12 -sh
novi pts/6 Sat 8pm 17 52 -bash
Data Assessment: Procedure

File date/time stamps
ls -alRu /mnt/floppy/utime
ls -alRc /mnt/floppy/utime
ls -alR /mnt/floppy/utime

Network ports
netstat -anp

Active Internet connections (servers and established)
Proto Local Addr Foreign Addr State Program
TCP 10.17.0.110:22 10.1.0.90:51327 LISTEN 28644/sshd
TCP 127.0.0.1:25 0.0.0.0:* LISTEN 1840/sendmail
TCP 0.0.0.0:32768 0.0.0.0:* LISTEN 1456/rpc.statd
TCP 0.0.0.0:68 0.0.0.0:* LISTEN 1363/rpc.statd
UDP 0.0.0.0:111 0.0.0.0:* LISTEN 1436/portmap
UDP 0.0.0.0:32768 0.0.0.0:* LISTEN 1456/rpc.statd

Collect system configuration
- Check for sniffers: ifconfig
- /etc/passwd, /etc/shadow, /etc/group
- Scheduled jobs: cron and at
- System init files: /etc/inittab, /etc/rc.d

Collect system log files
- Login logs in /etc/utmp, /etc/wtmp
- Check /etc/syslog.conf
- Log files in /var/adm, /var/log
- Process accounting files in /varacct
- Shell history files, e.g., ~/.bash_history
Preserve Evidence

- In-depth live system investigation
- Construct a bit-level copy of entire hard disk or partition for forensic examination
  - Create image in single-user mode
    ```bash
    md5sum /dev/hda
dd if=/dev/hda conv=noerror,sync | ssh desthost "cat >disk.img"
desthost> md5sum disk.img
    ```

Eradication

1. Do nothing
2. Kill attacker's processes and/or accounts
3. Block attacker's network access to system
4. Patch and repair what you think was changed, then resume operation
5. Investigate until root cause discovered, then restore system from backups and patch security holes
6. Call law enforcement before proceeding further

Follow-Up

- File reports with law enforcement, vendor, or regulatory agency
- File insurance claims if relevant
- Notify administrators of other affected systems
- Disciplinary actions against employees for internal attacks
- Update security of computer networks/systems
- Review handling of the incident
- Update incident handling policy/training
Counterattacking

Use legal procedures
- Collect chain of evidence so legal authorities can establish attack was real
- Check with lawyers for this
  - Rules of evidence very specific and detailed
  - If you don't follow them, expect case to be dropped

Technical attack
- Goal is to damage attacker seriously enough to stop current attack and deter future attacks

Consequences

1. Counterattack may harm innocent party
   - Attacker may have broken into source of attack or may be impersonating innocent party
2. Counterattack may have side effects
   - If counterattack is flooding, may block legitimate use of network
3. Counterattack antithetical to shared use of network
   - Counterattack absorbs network resources and makes threats more immediate
4. Counterattack may be legally actionable

Example: Counterworm

- Counterworm given signature of worm
- Counterworm spreads rapidly, deleting all occurrences of original worm
  - example: Welchia/Nachi hunts Blaster/MyDoom worms
- Issues
  - How can counterworm be set up to delete only targeted worm?
  - What if infected system is gathering worms for research?
  - How do originators of counterworm know it will not cause problems for any system?
  - And are they legally liable if it does?
Key Points

1. Security incidents come in many forms
2. Prepare for an incident before one occurs
3. Understand your response goals
4. Don’t trust the affected system in any way
5. Know your available data sources and their uses
6. Save data offline for later analysis
7. Legal issues of counterattacks
8. Phases of Incident Response:
   - Preparation, Identification, Containment
   - Damage Assessment, Preserve Evidence
   - Eradication, Recovery, Follow-up

References