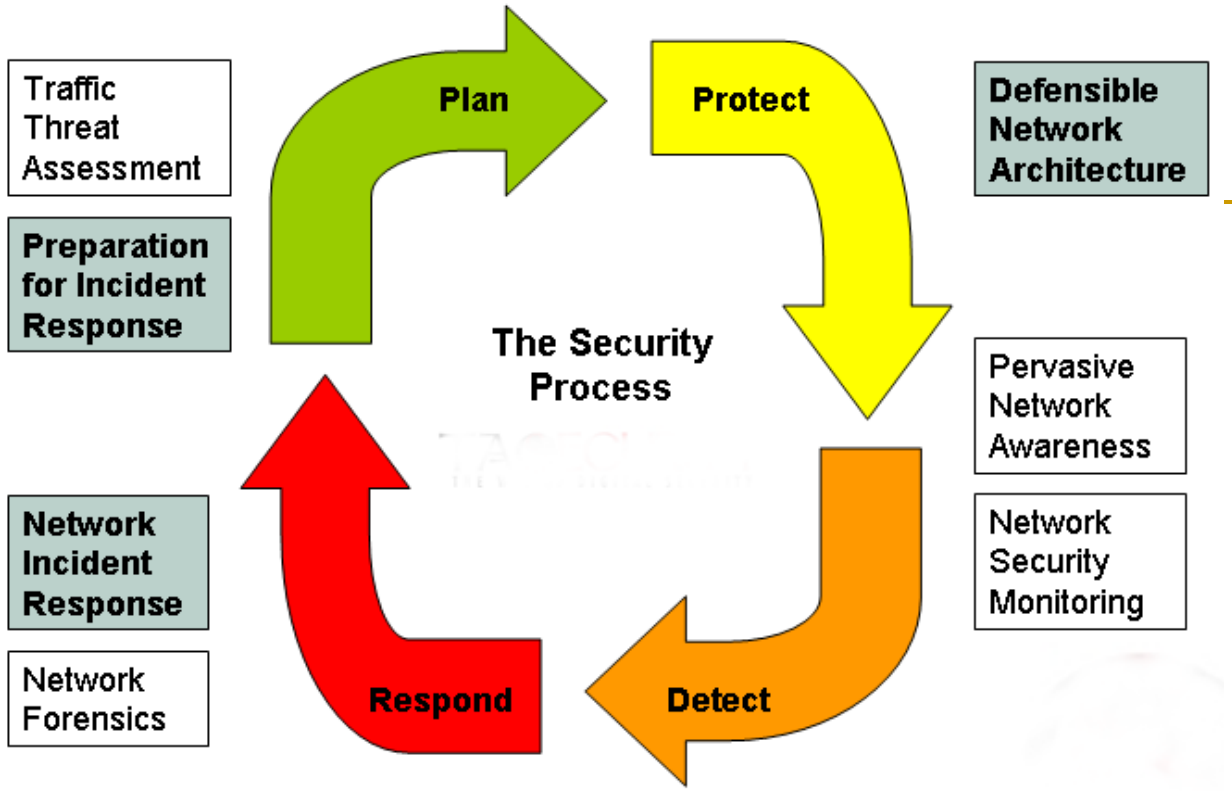
Chapter 1

Real World Incidents



Ed Crowley

Spring '10

Topics

- Relevancy
- Issues
- Incident Response
- Invita Case Study

Relevancy

- Increasingly, computer based evidence is involved in court.
  - Both civil and criminal.
- Increasingly, computer based evidence is involved in corporate decision making.

- Given the pervasive nature of computers and networks, we should expect this trend to continue.

Issues

- How can relevant digital information be obtained to support:
  - Criminal and Civil Court issues
  - Corporate Decisions
    - Disciplinary actions
- Who is responsible for obtaining this information?
- Significant Roles
  - Law enforcement?
  - System administrators?
  - Legal counsel?
  - Business managers?
  - HR?

Response Dimensions

- Legal
- Political
- Business
  - Sociological
- Technical

- Note that the technical investigation is only one of many response dimensions.

International Aspects: Invita

- Alexy Ivanov and Vasily Gorshkov, *10 Nov 2001*
- “Interview” at Invita headquarters recorded by FBI on videotape
  - Pair’s computer activities recorded with a keystroke logger.
  - Hacks focused on unpatched IIS and SQL Server Systems at financial institutions

`http://archives.neohapsis.com/archives/isn/2001-q2/0317.html`


msnbc

Home » News » Internet Underground

um of News

ts

FBI agent charged with hacking

Russia alleges agent broke law by downloading evidence

By Mike Brunker

MSNBC

Invita uilized MDAC vulnerability. References include:

http://www.msnbc.msn.com/id/3078784/

http://www.cybercrime.gov/gorshkovconvict.htm

http://cyb3rcrim3.blogspot.com/2006/03/our-fourth-amendment.html

http://www.crime-research.org/news/2002/08/Mess1801.htm

http://www.americanmafia.com/Feature_Articles_270.html

Traditional Hacks

- Servers and related resources are valuable.
  - For example, a server may have value as FTP servers for wares or other digital assets.
- Goals may include stealing:
  - Bandwidth
  - Storage
  - Similar resources
- Goals may also include launching attack against a third party.

Relevant Web Server Hack Issues

- Was source code or other sensitive information compromised?
- Did Internet users upload malicious code or modify source code?
- Was the computer accessed in any way?
  - If so, did the access occur at a higher privilege level?
  - Was the Computer used to access other systems in the DMZ?
- Was customer data present in the DMZ and accessible from the compromised server?

Questions?

Chapter 2

Introduction to the Incident Response Process

Ed Crowley

Spring '10

Topics

- Computer Security Incidents
  - Incident Examples
- Civil and Criminal Implications
- Incidence Response
  - IR Goals
  - IR Teams
  - Major IR Teams
  - Pre-incident Preparation
- Incident Detection
- Critical Incident Details
- Response Strategy
- Actions
- Incident Investigation
- Forensics
- Incident Resolution

Computer Security Incidents

- A computer security incident is:

  Any unlawful, unauthorized, or unacceptable action that involves a computer system or a computer network.

- Increasingly, they also refer to incidents involving other digital devices such as:
  - PDAs
  - Phones
  - Other
- Subject to Digital Forensics

Security Incident Examples

- Theft of trade secrets
- Email spam
- Harassment
- Unauthorized or unlawful intrusions
- Embezzlement
- Possession or dissemination of child pornography
- Denial of service (DOS) attacks
- Tortuous interference of business relations
- Extortion
- Any unlawful action when the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes.

Law Violations

- Many computer security incidents include public law violations
- May also be actionable in criminal or civil proceedings.

Incident Response Goals

- Prevent a disjointed, noncohesive response.
- Confirm or dispel whether an incident occurred.
- Promote accumulation of accurate information
- Establish controls for proper retrieval and handling of evidence.
- Protect privacy rights established by law and policy
- Minimize business and network operation disruption
- Facilitate criminal or civil action against perpetrators
- Provide accurate reports and useful recommendations
- Provide rapid detection and containment.
- Minimize exposure and compromise of proprietary data
- Protect organization's reputation and assets
- Educate senior management
- Promote rapid detection and/or prevention of such future incidents

Incident Response Team (CSIRT)

- Incident response, a multifaceted process contains:
  - Legal attributes
  - Technical attributes
  - Business attributes
  - Other attributes
- CSIRT
  - Responds to any computer security incident.
  - Normally, team is dynamically assembled when it is required.

Seven Major IR Components

1. Pre-incident prep and planning
2. Incident detection
3. Initial response
4. Formulate response strategy
5. Investigate the incident
6. Reporting
7. Resolution

Pre-incident Preparation

- Key
- Many computer security incidents are beyond our control
- As investigators, we have no idea when the next incident will occur.
- In nature, IR is reactive

Preparation

Organizational

- Security measures
- Intrusion detection system(s)
  - Host and/or network based
- Strong access control
- Timely vulnerability assessments
- Backups and restore capability
- End users training

CSIRT

- Appropriate policies and operating procedures
- Staff and employee training
- Documentation
- Jumpkit
- Hardware
- Software

Incident Detection

- Normally, computer security incidents are identified when someone suspects that an unauthorized, unacceptable, or unlawful event has occurred involving an organization's computer networks or data processing equipment.
- Pertinent initial response facts should be recorded via a checklist.
- See:

http://www.digi4nsic.com/incident_response/Incident%20Respo

Critical Incident Details

- Current time and date
- Who/what reported the incident
- Nature of the incident
- When the incident occurred
- Hardware/software involved
- Points of contact for involved personnel

Initial Response

Goal:

- Obtain enough information to determine appropriate response
  - Document steps needed to be taken.
  - Review and collect network based and other evidence.
  - Interview sys admins and business personnel
  - Review Intrusion Detection system
- At a minimum, the team must verify that an incident has actually occurred.

Formulate a Response Strategy

Goal

- Given the instant circumstances, determine most appropriate response strategy.

Considerations

- System criticality
- Information sensitivity
- Potential perpetrators
- Public knowledge
- Level of unauthorized access
- Attacker skill level
- System downtime
- Dollar loss

Response Strategy

- Details obtained during the initial response can be critical when choosing a response strategy.
- Response posture is capacity to respond, determined by technical capabilities …

Incidents and Possible Responses

- DoS Attack – Reconfigure router
- Unauthorized use – Possible forensic duplication
- Vandalism – Monitor web site. Repair web site.
- Theft of Information – Public affairs statement. Forensic duplication. LE contact.
- Computer intrusion – Monitor attacker activities. Isolate and contain scope of unauthorized access

Response Strategy Considerations

- Estimated dollar loss
- Network downtime
- User downtime
- Legal implications
- Public implications
- IP theft
- Operational impact

Possible Actions

Legal

- Civil or criminal?
- Likely action will achieve desired outcome?
- Incident cause established?
- Appropriate documentation?

Administrative

- Reprimand letter
- Dismissal
- Mandatory leave of absence
- Reassignment of job duties
- Temporary reduction in pay
- Public/private apology
- Withdrawal of privileges

Incident Investigation

- Incident's investigation phase involves determining
  - Who
  - What
  - When
  - Where
  - How
  - Why
- Two investigation phases.
  1. Data collection
  2. Forensic analysis

Data Collection

- Accumulation of facts and clues that should be considered during forensic analysis.

Challenges

- Must be done in a forensically sound manner
- Often huge amounts of collected data
- Evidence must be handled appropriately

Host Based Information

Includes logs, records, documents, and any other information…

Volatile information includes:

- System date and time
- Applications currently running
- Established network connections
- Currently open sockets (ports)
- Applications listening on the open sockets
- State of the network interface (promiscuous or not)

Live Response

- Conducted with the system powered on and running
- Initial live response
  - Obtains only volatile data
- In-depth live response
  - Volatile data plus logs
- Full live response
  - All data collected
- At some point, decision will need to be made whether, or not, to perform a forensic duplication

Network Based Evidence

- IDS logs
- Consensual monitoring logs
- Nonconsensual wiretaps
- Pen register/trap and traces
- Router logs
- Firewall logs
- Authentication servers

Network Surveillance

- Confirm or dispel suspicions surrounding an incident.
- Accumulate additional evidence and information
- Verify the scope of a compromise
- Identify additional parties involved
- Determine a timeline of events occurring on the network
- Ensure compliance with a desired activity

Forensic Analysis

Includes reviewing all collected data.

- Consists of three phases
  1. Forensic Duplication*
  2. Prep Data
  3. Analyze Data

* http://homepage.cs.uri.edu/courses/fall2005/hpr108b/MD5_case.html

** http://www.cftt.nist.gov/

**NIST Forensic Tools

Data Preparation Process

From the Working copy

1. Create file lists
2. Recover deleted data
3. Recover Unallocated space
4. Perform statistical data Partition Table File System
5. Perform file signature analysis
6. Identify known system files

Data Analysis

- Extract email and attachments
- Review installed applications
- Search for relevant strings
- Perform software analysis
- Perform file by file review
- Review browser history files
- Review data collected during live response
- Review all the network based evidence
- Identify and decrypt encrypted files
- Perform specialized analysis

Reporting

- Can be the most difficult phase
- Document immediately
- Write concisely and clearly
- Use a standard format

Two resolution phase goals

1. Implement host and/or network based and procedural countermeasures to prevent an incident from causing further damage and
1. Return your organizational to a secure, healthy operational status.

10 Incident Resolution Steps

1. Identify organization's top priorities
2. Determine nature of the incident
3. Determine if there are underlying or systemic incident causes
4. Restore any affected or compromised systems
5. Apply corrections required to address host based vulnerabilities

1. Apply network based countermeasures
2. Assign responsibility
3. Track progress
4. Validate that all remedial steps or counter measures are effective
5. Update your security policy and procedures.

Questions?