Practical Windows Forensics

Lora Fulton lfulton@bu.edu
Eric Jacobsen jacobsen@bu.edu

July 20, 2001

MIT Security Camp

BOSTON UNIVERSITY

Overview

- BU is building its toolkit for Windows security incident handling.
- We will attempt to share what we've learned about doing forensics in the Windows environment.

Agenda

- Windows at Boston University
  - Who we once were
  - Why we felt we needed to change
  - What we've changed
- Our Windows Forensics procedures
  - Goals
  - What we do
- Questions and Comments

BOSTON UNIVERSITY

History

- M$ Windows at BU, prior to 2001.
  - Limited experience with Windows servers, still perceived as a desktop operating system.
  - Security responsibilities pushed off to local systems administrators.
  - "We will deal with problems as they come up."
  - No interest in forensics, just fix the problem and move on.

Impetus to Change

- Victims of our Residential Networking (ResNet) Initiative were flooding our abuse/security mail queues with complaints.
- Arrival of BackOrafice/Sub7 trojans with potential to do great harm inside our firewall.
- Administrative push towards Exchange servers, Terminal servers, Active Directory services.

Impetus to Change

- Hardware vendors shipping products with Windows based components (Xerox printers, IBM ESS, Card Access systems, e.g.)
- Public terminal rooms with Windows desktops

Changes

- Added Lora Fulton to the full-time security staff.
- Build information distribution channels for Windows security information.
- Develop an understanding of what needs to be done to secure a Windows system.
- Efforts to promote Virus Protection for all Windows systems.
- Adapt existing Unix Forensics checklist to the Windows platform.

Forensics Goals

- Our methods are not intended to collect evidence for law enforcement, just for our own education.
- Reduce the amount of time required to conduct an investigation (and therefore freeing a system up for repair work quicker).
- Ability to identify widespread problems so we can notify our community about them (identification of an attack signature or footprint).

Basic Procedure

- Follow checklist, collect all data from system(s)
- Interview with systems administrator / primary users
- Analyze available data to determine source and method of attack
- Apply information to detect other compromises

Preparation

- Try to have a theory of what happened before investigating the system.
- Don't show your cards to others.
- Don't show your cards to yourself
  - Prove what happened, not what you think happened. (Don't believe your own theories)

Pre-inspection Procedures

- Make Appointment
  - Meeting place/directions
- Admin account and password
- List of intended uses
  - File/Pint/Web/FTP/DC/PDC/TS/Desktop

Gather Tools

- Clip board
  - New checklists
  - Scratch paper (no notebooks – unless for LE)
  - Sample srvinfo and pstat printouts
- Tool Kit
  - CD case with pockets
  - Spare floppies/zip disks , blank disk labels
  - Copy of srvinfo, fport, plus any other tools you like
  - Service Packs/**Resource Kit**/ Other CDs

System Information & Basic Configuration

- Hostname, IP Address (ipconfig /all or srvinfo)
- System Location, Owner, Administrator
- Hardware Platform, CPU type
- Operating System, including service pack (winver or srvinfo)
- Hot Fixes Applied (add/remove programs)
- Anti-Virus Software (installed/updated)

Date & Time / Disk Layout

- Date & Time Zone
  - Compare to a wristwatch and record difference
- Uptime (srvinfo again)
- What drives and shares are present
  - Local Disks/Networked Drives
- What File System Type is being used
  - NTFS/FAT/FAT32

System Services

- Processes
  - Task Manager / Processes Tab
  - save to bitmap using paint from accessories
  - pstat from Microsoft's Resource Kits
- Services
  - netstat –an >c: \temp\hostname\netstatlog.txt
  - more c:\temp\hostname\netstatlog.txt
  - fport (foundstone.com)
    - tcp/ip process to port
  - srvinfo again

System Logs

- Event logs
  - Are they enabled?
  - Review and take copy if possible
- Auditing
  - Never enabled?
- IIS/FTP logs
- Are they even being read?

Unauthorized Changes

- Search for changes to files
  - Search for files modified & created by date
    - W2k=Search NT=Find (from start menu)
  - Search for hidden files & folders
    - dir /S /ah >c:\temp\hostname\dirahout.txt
    - edit c:\temp\hostname\dirahout.txt & search on date
- Search for changes to the registry
  - DumpReg (Somarsoft.com) – only if sure of date
    - Able to sort by modified time on NT systems
    - Option to only show keys changed since date

Other

- Copy of users & groups
  - Export lists in W2K & showmbrs from RK
  - User Manager in NT4 (clipboard to paint trick)
- Check temp files (c:\winnt\temp, c:\temp, etc)
- Zip copy of c:\temp\hostname folder
- Intended use(s)
- Remote port scan

Findings

- What did they do with the system?
  - Trojan Software
  - Added Hidden (or non-hidden) directories
  - Added new accounts
  - Cracking the SAM

Summary

- Is the system compromised?
  - At what privilege level?
- Via what mechanism?
- When did the compromise first occur?
- Where did the intruders come from?
- Where else did they attack from here?

Follow-up

- Incident Reports
- User/Admin educational opportunity
- Chance to promote usage of central resources
- Update Incident Database
- File all notes/disks, etc – in safe place

Questions and Comments

- This is a work in progress. We invite your feedback.
- lfulton@bu.edu Subject: Security Camp / Windows Checklist

BOSTON UNIVERSITY