

Novell Netware OS Forensics

Lab Assignment Number 1

Background Information

Novell Netware is a commonly used Network operating system that is popular in the education and medical fields for its ease of administration and off server capability. Although Novell is currently replacing the Netware OS with a Linux variant it is still commonly used and therefore a forensics technician should have some experience with the OS.

As stated above the administrator and the forensics technician will do the majority of work off console. Minimizing contact with the server due to the vastly superior remote management capabilities and the less than adequate GUI on the server itself.

Lab Tech Requirements:

For this exercise students will work in teams of 2 as one computer is required for hosting the server and one is required for client connection, however as a result students will complete two exercises the first being a live response event and the second a forensics re-construction

For each group of 2 students the following will be required:

- One Computer designated to be the server
 - Installed VMWare server
 - Novell Server Virtual image

- One Computer Designated to be the client machine:
 - Installed Windows XP OS with Novell Netware client, console 1
 - OR
 - Vmware Server with windows Novell workstation image

- Computers be connected to a small switch isolated from a outside network

- Server image is preconfigured to have IP address 172.16.0.6, 255.255.0.0
- VMware workstation image is preconfigured to have IP address 172.16.0.7, 255.255.0.0
- If using real hardware workstations must be configured to IP address 172.16.0.7, 255.255.0.0

Scenario 1

You are a contracted technical security specialist for a large company in Ontario Canada, the company that you work for provides incident response and technical support for a large number of fast food restaurants in Canada, each restaurant is equipped with a small Novell server for managers to access information and print reports, manage schedules and surf the internet. Upon sending a message to another user Mr. Bob Manager at one of the restaurants notices an unusual user connected to the server, following established procedures he informs the helpdesk and the incident is identified as a live attack happening on the server currently. You are dispatched to the site and must complete a live recovery on the Netware toolkit. Use the Netware security knowledgebase at www.theforcenet.ca/novell for assistance in performing your live recovery

Scenario 1: Deliverable Requirements

- A fully completed live response worksheet documenting all the steps outlined in the live response knowledgebase article.

Scenario 2

After completing your live analysis of the server in question Mr. Bob Manager informs you that there may be a user on the system with child pornography on his or her home directory, after briefly looking through the users home directories using your admin account you discover there is no picture files on any of the users home directories however Bob is insistent on the fact that Joe B Donuts (a recent addition to the management staff) is looking up child pornography on his workstation during the night shift. After calling your supervisor you are instructed to investigate the matter.

Scenario 2: Deliverable requirements

- A floppy disk containing 3 recovered images from Mr. Donuts home directory
- A report with screenshots outlining the steps taken and the methodologies used for forensics recovery on the Netware server.