Unit OS A: Windows Networking

A.4. Lab Manual

Roadmap for Section A.4

Lab experiments investigating:

- Listing registered winsock transports
- Viewing named pipes and named pipe activity
- Investigating NetBIOS names
- Watching TDI activity
- Listing loaded NDIS miniports
- Capture network packets with network monitor

3

List Registered Winsock Transports

- Winsock integrates with the Windows I/O model and uses file handles to represent sockets
  - Kernel-mode Ancillary Function Driver (AFD - \Windows\System32\Drivers\Afd.sys) implements socket-based functions
  - AFD is a TDI client and executes network socket operations by sending TDI IRPs to protocol drivers
  - AFD isn't coded to use particular protocol drivers; user-mode Msafd.dll informs AFD of the name of the protocol used for each socket
  - AFD opens the device object representing the protocol
- **Windows Sockets Configuration(Sporder.exe)** utility shows registered Winsock transport providers

4

Viewing Named Pipes and Named Pipe Activity

- Run Pipelist (Sysinternals) to see the named pipes on a system
- Run Filemon (Sysinternals) to watch named pipe activity in real-time

5

Investigating NetBIOS names

- NetBIOS relies on a naming convention
  - computers and network services are assigned a 16-byte name called a NetBIOS name
  - Only one instance of a unique NetBIOS name can be assigned to a network
  - A client can broadcast messages by sending them to a group
- Windows automatically defines a NetBIOS name for a domain
  - the first 15 bytes of the left-most DNS name
  - support interoperability with Windows NT 4 systems as well as Consumer Windows
- **Nbtstat.exe -n** shows NetBIOS-to-TCP/IP mappings

6

Watching TDI Activity

- Run TDIMon (Sysinternals) to watch TDI activity
  - Access any network resource
  - TDImon sees every IRP that TDI clients issue to network protocols.
  - By intercepting TDI client event callback registration, it also monitors event callbacks.

7

Listing Network Driver Interface Specification (NDIS) miniports

- NDIS-conforming network adapter drivers are called NDIS miniport drivers
  - NDIS library (\Windows\System32\Drivers\Ndis.sys) implements the NDIS boundary that exists between TDI transports (typically) and NDIS drivers
  - a helper library that NDIS driver clients use to format commands they send to NDIS drivers
- Kernel debugger shows miniports:
  - !miniports and !miniport commands
  - ndiskd extension needs to be loaded

8

Using Network Monitor to Capture Network Packets

- Note: requires Windows 2000 Server or higher
- Install Network Monitor Tools
- Configure Network Monitor to attach to a network connection
- Run Network Monitor (netmon.exe)
- Press go to begin monitoring
  - Perform network activity
- Press stop to stop monitoring
- Double-click on monitor event to reveal more information

9