Network Administration Tools

Module 9

Types of Networking Tools

- Configuration
  - Addressed in previous modules
- Diagnostic
  - Host troubleshooting
    - Network status
    - Connectivity
  - Packet analysis
- Security Testing
  - Profiling
  - Vulnerability Assessment

Network Status Tools

- Reviewing configuration utilities and files are helpful, but
  - These tells us how things should be configured
  - Incorrect entries or remote dependencies (ex. DHCP) may be contributing to a problem
  - Troubleshooting requires knowing what the system is actually using for key parameters and what it is experiencing

Ifconfig/ipconfig

- Unix uses ifconfig, Windows uses ipconfig
  - Tools tell us:
    - Driver sees the network
    - Type of physical layer connection
    - MAC address
    - Ip address, netmask and broadcast address
  - Tools can manipulate the interface if needed
    - Renew DHCP lease
    - Reset an interface or take it offline

netstat

- Used in both Unix and Windows
- Tells us:
  - Interface statistics – (netstat –i)
  - Routes and related status– (netstat –r)
  - Listening sockets and connections' status (netstat –a)
  - Network protocol statistics (network –s)

Network Connectivity Testing

- These tools help answer:
  - Why doesn't browsing work?
  - Why doesn't browsing to a new URL work?
  - Why doesn't browsing to a site accessed yesterday not work?
- Different tools are needed to isolate source of problem, some sources
  - User error
  - Local system
  - Local network
    - Internet connectivity
    - Security controls
    - Server side issues

Network Connectivity Testing

- Layer 1 – Cable tester, link light
- Layer 2 – arp – command line tool
- Layer 3 :
  - ping – command line tool
  - traceroute/tracert – command line tool
  - pathping – Windows command line tool
  - dig or nslookup – name resolution
- Layer 4:
  - nc or netcat – 3rd party command line tool

Network Connectivity Testing

- Layer 7 / Application Layer:
  - Testing this layer is more about functionality testing than connectivity
  - Application layer protocols are very different from each other, so testing tools are specialized to the network service
    - ASCII based protocols can be manually tested using nc or telnet
      - This requires understanding the protocol and the service software's support for the protocol

Layer 2 Testing

- Issues at this layer result in being unable to communicate with peers on same LAN
  - First router between system and destination is a peer on the system's LAN
- arp is a tool on Unix and Windows
  - Capabilities vary
  - Both will display ARP entries
    - Connectivity with a peer is impossible without a valid ARP entry for the peer

Layer 3 Testing

- Issues at this layer result in not being able to communicate with local peers and distant devices/hosts
  - A wrong IP address for destination will appear as a connectivity issue
- ping uses ICMP to elicit a response from destination
  - Some devices are configured not to respond for security reasons

Layer 3 Testing

```
ping www.iastate.edu
PING www.iastate.edu (129.186.23.166): 56 data bytes
64 bytes from 129.186.23.166: icmp_seq=0 ttl=241 time=69.179 ms
64 bytes from 129.186.23.166: icmp_seq=1 ttl=241 time=67.770 ms
64 bytes from 129.186.23.166: icmp_seq=2 ttl=241 time=67.606 ms
64 bytes from 129.186.23.166: icmp_seq=3 ttl=241 time=79.709 ms
64 bytes from 129.186.23.166: icmp_seq=4 ttl=241 time=70.331 ms
64 bytes from 129.186.23.166: icmp_seq=5 ttl=241 time=70.583 ms
64 bytes from 129.186.23.166: icmp_seq=6 ttl=241 time=71.797 ms
64 bytes from 129.186.23.166: icmp_seq=7 ttl=241 time=68.080 ms
64 bytes from 129.186.23.166: icmp_seq=8 ttl=241 time=71.250 ms
^C
--- www.iastate.edu ping statistics ---
9 packets transmitted, 9 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 67.606/70.701/79.709/3.498 ms
```

Layer 3 Testing

- Incorrect routing tables, routing filters, device failure, link failure/congestion are possible sources of the problem
  - ping will fail if ICMP is blocked or responses are disabled or any of the issues listed above
  - Need a tool to give visibility to what may have happened between source and destination
- traceroute/tracert – traditionally uses UDP or ICMP – default is commonly UDP

Layer 3 Testing

traceroute -n -P ICMP www.iastate.edu
traceroute to www.iastate.edu (129.186.23.166), 64 hops max, 72 byte packets
 1 192.168.1.1 1.378 ms 0.995 ms 0.976 ms
 2 192.168.2.1 2.003 ms 1.581 ms 1.796 ms
 3 * * *
 4 216.161.116.211 28.485 ms 26.078 ms 33.812 ms
 5 75.160.210.145 25.462 ms 24.468 ms 30.098 ms
 6 67.14.8.190 38.602 ms 38.094 ms 37.827 ms
 7 63.146.27.18 40.842 ms 37.424 ms 39.801 ms
 8 4.69.138.158 65.118 ms 63.667 ms 63.905 ms
 9 4.69.132.61 66.002 ms 65.794 ms 66.052 ms
10 4.69.135.237 66.581 ms 70.097 ms 63.157 ms
11 4.53.34.14 72.821 ms 99.630 ms 69.965 ms
12 192.245.179.49 74.236 ms 79.970 ms 80.018 ms
13 129.186.254.139 80.120 ms 68.682 ms 71.121 ms
14 129.186.23.166 69.414 ms 67.602 ms 67.351 ms

Layer 3 Testing

- Name resolution can be source of error
- Use dig or nslookup to verify the destination's domain name can be resolved.
- Working with IP addresses during troubleshooting avoids relying on DNS resolution, which may not be working while the problem is being resolved.

Layer 4 Testing

- Assumes lack of access to destination administrator or operating condition
  - Knowing whether a service is listening to the TCP or UDP port expected requires probing
- The tool nc (also called netcat) or ncat can make TCP connections and direct UDP packets to specified ports

Packet Analysis

- Operational or security problems are at times best understood by knowing what is actually being sent on the channel.
- The layered network stack of a host hides the details as encapsulation is stripped away.
- Tools are needed that can reveal the transmitted bits within frames.

Packet Analysis

- At 100 Mbps or 1 Gbps Ethernet, several minutes of capture is potentially a large volume of data
- Analysis of the packets may reveal unexpected protocols or protocol behavior, unusual or unexpected parameters or payload.
  - Interpretation requires an understanding of the protocols and the context

Packet Analysis

- Packet – fundamental data structure within IP networking based data transfer
- Network analyzers capture frames, Layer 2, by instructing the NIC to operate in “promiscuous” mode.
- Packet analysis tools apply protocol standards to captured frames to aid in analysis.

Packet Analysis

- Tools
  - tcpdump – common Unix tool run at command line
  - wireshark – GUI Windows and Mac OS X tool
    - Much more sophisticated than tcpdump

Security Testing - Profiling

- Profiling tools help administrators understand the attack surface a host presents to the network
  - Attack surface – the collection of a host's exposures or opportunities, which illegitimate users can use to carryout malicious activity
    - Rock climbing requires defects on the rock face on which to place pitons, hands and feet. If the defects are sturdy, a climber put their weight on the piton or hand or foot in order to climb.
    - A completely smooth and hard steep surface is very hard to climb

Security Testing - Profiling

- Each service listening for packets is an exposure
  - A service may impede malicious activity by:
    - Requiring challenging authentication
    - Requiring encryption with certificates or keys very difficult to obtain
    - Being secure service software invulnerable to protocol or service usage abuses
    - Implementing IP address based access control
  - Host's underlying TCP/IP stack needs to be immune to protocol abuses as well

Security Testing - Profiling

- Safer to assume illegitimate and legitimate users can access the same network
  - Providing a service to a legitimate user exposes the host to processing packets from any source able to direct packets to the network on which it is listening.

Security Testing - Profiling

- Tool
  - nmap is a tool for Unix and Windows
    - Pings a range of addresses
    - Determines services running on TCP and UDP ports
      - Service identification may be difficult, but nmap can determine if something is servicing a port.
    - Identifies the OS by analyzing the replies made by target by analyzing protocol parameter usage
      - Standards allow for some flexibility in implementation, which results in OS developers introducing idiosyncrasies

Security Testing - Profiling

- Profiling a system is helpful for operations
  - Means to remotely inventory services
  - Unexpected changes in profile may be helpful in troubleshooting

Security Testing – Vulnerability Assessment

- Profiling reveals the attack surface
- Vulnerability scanning explores each exposure looking for known issues or possible concerns.
  - Exploration involves interacting with the service listening to the port
  - Exploitation of a vulnerability is many times avoided because there is a greater risk of operational issues resulting from the test.

Security Testing – Vulnerability Assessment

- Tools
  - Nessus
  - Metasploit
  - OpenVAS
- Vulnerability scanning results need thorough analysis
  - Some vulnerabilities are suspected, but may not be present on a particular host