CMSC 449
Malware Analysis

Lecture 6

Network-Based Dynamic Analysis Tools

Network-Based Dynamic Analysis Tools

- Important for analysts to be able to inspect a malicious file’s network traffic

- Malware often uses the network for:
  - A first-stage downloading a payload
  - Connecting to a C&C server

- Malware will often sleep or exit if it cannot reach the internet

FakeNet-NG

- Tool that “fakes” that a VM is connected to the internet

- Redirects network traffic to listeners for common protocols
  - HTTP/HTTPS
  - DNS
  - SMTP
  - Many other protocols supported

- Can configure custom listeners if needed

FakeNet-NG

- Listeners will give a valid response to the malware
  - Better than saying “no internet connection” and the malware exiting
  - Can customize how the listeners respond to the malware

- Captures network traffic sent to the listeners in a .pcap file
  - .pcap = Packet Capture file

- Can inspect the captured packets using a tool like WireShark

FakeNet-NG

- Instructions for setting up FakeNet-NG on your VM have been posted on Blackboard

- Make sure to take a snapshot before setting up FakeNet-NG!
  - It messes with your VM’s DNS server
  - Much faster to revert to snapshot than try to fix it

FakeNet-NG Setup Demo

Wireshark

- Tool for analyzing network traffic

- Can inspect network traffic live, or open a .pcap file

- Tons of features for querying, interpreting contents of packets

Netstat Command

- Command-line tool that lists existing network connections

- Flags allow the command to show information such as:
  - Name/PID of the process
  - State of the connection
  - Source/destination IP and port

- `netstat -abn`

Wireshark and Netstat Demo

PMA Lab 7-2