Final Review, Part 2

Worms

- Propagation methods
  - Random
  - Hitlist
  - Tree-structure hitlist
- Worm countermeasures
  - Honeypots
  - Tarpits
  - Network telescope

Code Analysis

- Taint Analysis
  - c = a + b
- Symbolic Execution
  - Know what a ‘path’ is
    - A path is a path even if it is not feasible

Path Analysis Example

```
char choice = determine_choice();
   if (choice == 'n')
               ...       // Branch 1
   if (choice == 'y')
               ...       // Branch
```

Path 1: Branch 1 ^ Branch 2 ::: choice == 'n' ^ choice == 'y'

Path 2: Branch 1 ^ ! Branch 2 ::: choice == 'n' ^ choice != 'y'

Path 3: ! Branch 1 ^ Branch 2 ::: choice != 'n' ^ choice == 'y'

Path 4: ! Branch 1 ^ ! Branch 2 ::: choice != 'n' ^ choice != 'y'

Firewalls and IDS

- What is the difference?
  - Active vs. Passive
- What do firewall rules look like?
  - Allow/drop protocol ip:port -> ip:port
  - Allow tcp *:* -> 1.2.3.4:25
- Filter by interface
  - Allow tcp *:*/out -> 1.2.3.4:25/in

Web Security

- Cross site scripting
  - A malicious server attacking a victim server with the help of a victim client.
  - The malicious server supplies malicious code that the victim user then unwittingly injects into the victim server.
- HTTP Response splitting
  - A way to spoof web pages
  - Trick a server into returning a fake page
    - Relies on the server echoing user input