DENIAL OF SERVICE

RULES OF ENGAGEMENT AND MITIGATION STRATEGIES

Stuart Cianos, CISSP

SF Bay ISSA Meeting - March 12th, 2014

RULES OF ENGAGEMENT

- Be prepared:
  - Approach must cover all your bases
    - Vulnerabilities in the application stack
      - Time complexity: O(1), O(n), O(log n), O(n^2), etc.
        - *Example*: Attacks against hashing functions (collisions)
        - *Example*: Failing to enforce reasonable limits (shopping cart with 100,000 items)
      - Input validation and bounds checking
        - Can lead to injection vulnerabilities, buffer overflows, etc.
          - Can cause application to end abnormally.
          - Can have the side effect of remote code execution, theft of information, or worse.
      - Improper error handling
        - Application failures and/or undefined behavior
          - A multithreaded instance serving 25,000 concurrent users may have noticeable impact on abend.

RULES OF ENGAGEMENT

- Be prepared:
  - Approach must cover all your bases
    - Vulnerabilities in the network stack
      - Takes advantage of (typically) unintended nuances of the design of the networking stack.
      - Denial of Service
        - "Traditional"; a limited or readily identified set of attackers.
        - Typically utilizes the sheer force of a few
        - Harder to hide
          - GMC vs. Yugo
      - Distributed denial of Service
        - A diverse set of attackers, typically under C&C
        - Easy to hide
        - Sheer force of many united against a greater power
          - 50,000 Yugos vs. GMC

RULES OF ENGAGEMENT

- Know where your bodies are buried
  - Consider modeling your threat landscape
    - Introspect: Why is this system a target? What does this outfit have? Be the attacker and step into your adversary's shoes.
      - What does your victim have to offer?
        - Bandwidth? Money? Tools? Political Platform? Industrial trade secrets? Public Sentiment? Sabotage?
        - Do you have more to offer than angry customers?
          - ***Don't ever forget that a DDOS is a great diversion or opportunity for covert side channel.***
      - Why do you want it?
      - How are your going to get it?
      - How motivated are you to get it?
      - How will you get away with it?

RULES OF ENGAGEMENT

- Rule #1:
  - You have no control of outside entities
    - You cannot stop a denial of service attack

      but you can

      Mitigate a denial of service attack
      - Rule #2: Big lips sink ships. Do not engage attackers. Always maintain integrity.

- The goal is to make the target undesirable:
  - The cost of the attack is more than the target is worth (in time, money or both)
  - The target is not trivially vulnerable
  - The target has nothing to offer

MITIGATING DOS ATTACKS

- Since the flow of traffic cannot be stopped…
  - Work with the traffic and go with the flow
    - **Route**
      - Limited & identified sources? Upstream null route is effective.
      - During a DDOS attack, routing may be used to swing traffic to alternate data center(s) for capacity or scrubbing.
        - Not the same as pointing DNS at a proxy. If the attacker can determine the backend network behind the proxy, it's game over.
        - Using BGP to control where target AS is routed to.
      - Poor man's solution: Advertise DNS to filtering proxy
    - **Absorb**
      - Effective on its own if you have the capacity; neuters attack.
      - How quickly can capacity be adjusted on demand?
    - **Filter/Scrub**
- Defense must be layered
- **THINK SCALABILITY** in systems design
- **MAKE NO ASSUMPTIONS** of behavior

BUSINESS CONSIDERATIONS

- Budget ahead of time
  - Tool should be low cost to deploy and operate
  - Budget ahead of time; this should be a known COB
  - How long can the business survive offline?
    - Long term ramifications?
      - Loss of customer trust and faith
- Know the requirements
  - What is the expectation from brass?
    - Business continuity plan requirements
- Know the business and industry
  - Know what **capabilities** and resources are available
  - Know where **opportunities for improvement** exist