Jacadis
Strategic IT security solutions.

OISF

DDoS Attack Preparation and Mitigation

Jerod Brennen, CISSP

Principal Security Consultant, Jacadis

September 8, 2011

Agenda

Jacadis
Strategic IT security solutions.

- What is a DDoS attack?
- Why are these attacks launched?
- How do we prepare?
- How to we respond?
- Resources

DoS Attacks

Jacads
Strategic IT security solutions.

- Denial of Service
  - Network resources
  - Host resources
  - Application resources
- Types
  - ICMP Flood
    - Smurf attack
    - Ping flood
    - Ping of death
  - SYN Flood
    - SYN – SYN/ACK… Wait. Where's my ACK?
    - Unending knock-knock joke
  - Teardrop Attack
  - Low and Slow

DDoS Attacks

Jacads
Strategic IT security solutions.

- Distributed Denial of Service
  - Multiple sources
  - Traditional countermeasures don't work
- Types
  - Download entire site, repeat ad nauseum
  - Abuse SSL negotiation phase

Why Launch a DDoS Attack?

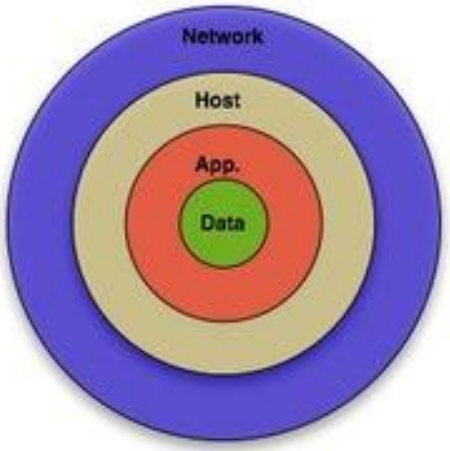
Jacads
Strategic IT security solutions.

- Motive
  - Extortion
  - Revenge
  - Hacktivism
  - Unintentional (@feliciaday)
- Means
  - Botnet
    - Infected machines
    - Voluntary
  - Availability of tools
    - Low Orbit Ion Cannon (LOIC) – TCP/UDP
    - slowhttptest – HTTP
- Opportunity
  - We're talking about the INTERNET…

Preparation

Jacads
Strategic IT security solutions.

- **Technical**: Defense-in-Depth
  - Network
  - Operating System
  - Web/Application Server (*)
  - Application



- **Procedural**: Security Incident Response
  - Policy
  - Procedures
  - Tabletop Exercises

Threats to your data never go away.
Neither should your security partner.
Making the unseen seen

Preparation – Network Architecture

Jacads
Strategic IT security solutions.

- Align with Cisco SAFE security reference architecture
- Deploy and tune tools
  - Intrusion Prevention System (IPS)
  - Security Information Event Management (SIEM)
  - Bandwidth Monitoring and Management
  - Anti-DDoS Hardware (*)
    - Cisco Guard / PreventTier
    - RioRey
- Evaluate IPv6 configurations

Preparation – Network Router

Jacads
Strategic IT security solutions.

- Enable Reverse Path Forwarding
  - `ip verify unicast reverse path`
- Filter all RFC-1918 address spaces
  - `10.0.0.0 - 10.255.255.255 (10/8 prefix)`
  - `169.254.0 – 169.254.255.255 (169.254/16 prefix)`
  - `172.16.0.0 - 172.31.255.255 (172.16/12 prefix)`
  - `192.168.0.0 - 192.168.255.255 (192.168/16 prefix)`
- Network Ingress Filtering, per RFC-2827
  - Drop forged packets
- Enforce rate limiting for ICMP and SYN packets

Preparation – Network Firewall

Jacads
Strategic IT security solutions.

- Deny private, illegal, and routable source IP's
  - 0.0.0.0
  - 10.0.0.0-10.255.255.255
  - 127.0.0.0
  - 172.16.0.0-172.31.255.255
  - 192.168.0.0-192.168.255.255
  - 240.0.0.0
  - 255.255.255.255

Preparation – Operating System

Jacads
Strategic IT security solutions.

- Harden the Host
  - Center for Internet Security
  - DISA STIG's
  - Vendor guides
- Patch
  - Automate the process
  - Trust, but verify
- Host Vulnerability Scans
  - DoS vulnerabilities

Preparation – Apache on Linux

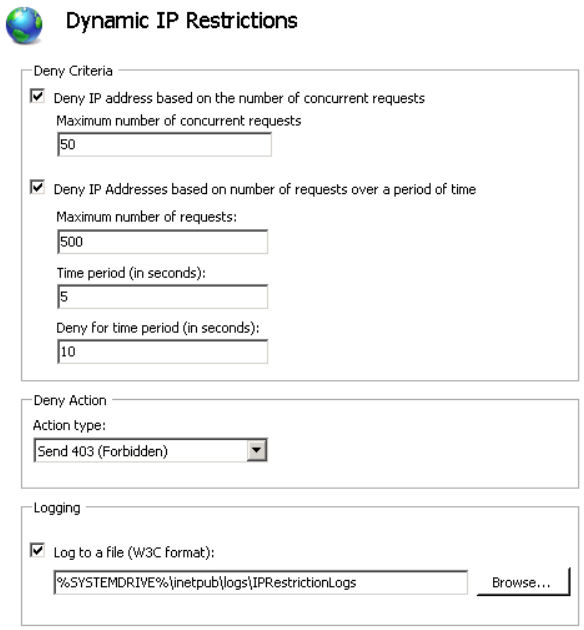
Jacads
Strategic IT security solutions.

- Advanced Policy Firewall (APF)
  - iptables (netfilter)
- (D)DoS Deflate
  - `netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n`
  - Automatically block attacking IP's
  - Automatically unblock IP's after x seconds
- Apache modules
  - mod_evasive
  - mod_security

Preparation – IIS on Windows

Jacads
Strategic IT security solutions.

- UrlScan
  - Integrate with IIS
  - Mitigate SQL injection attacks
  - Restrict potentially malicious HTTP requests
- Dynamic IP Restrictions
  - Requests over time
  - Deny action
  - Logging



Preparation – Application

Jacads
Strategic IT security solutions.

- Third Party Services
  - Akamai – Web Application Acceleration
  - Prolexic – Pipe Cleaner
- Load Balancers
  - Take advantage of virtualization
- Baseline Your Performance
  - Thresholds
  - Source IP reports
- Web Application Vulnerability Scan
  - DoS vulnerabilities

Preparation- Incident Response

Jacads
Strategic IT security solutions.

- Policy
  - Roles and responsibilities
  - Decision points
- Procedures
  - Step-by-step instructions
  - Critical contact information
    - ISP
    - Hosting provider
    - Law enforcement
- Tabletop Exercises
  - Practice!

Mitigation – Network

Jacads
Strategic IT security solutions.

- Log analysis
  - Understand the attack
  - `netstat, awk, grep`
- Contact your ISP
  - Drop attacking traffic before it hits any of your resources
- Null route attackers
  - `ip route 192.168.0.0 255.255.0.0 Null0`
- Implement your geographic IP rules
  - Deny all traffic from non-customer IP blocks
- Enable third party services/solutions
  - Temporary
  - Cost

Mitigation – Host and App

Jacads
Strategic IT security solutions.

- Add additional servers
  - Temporary
  - Again, take advantage of virtualization
- Tighten web app firewall rules
  - Based on attack pattern

Contact Law Enforcement?

Jacads
Strategic IT security solutions.

- Pros
  - Prevent future attacks against your org
  - Prevent future attacks against other orgs
- Cons
  - Attack becomes public record
  - Additional resources = time + money
- Decide in writing what action you will take before an incident occurs.

Resources

Jacadis
Strategic IT security solutions.

- Denial of Service Attacks Explained
  - CERT
    - http://www.cert.org/tech_tips/denial_of_service.html
  - Wikipedia
    - http://en.wikipedia.org/wiki/Denial-of-service_attack
- RFC's
  - RFC-1918 – Address Allocation for Private Internets
    - http://tools.ietf.org/html/rfc1918
  - RFC-2827 – Network Ingress Filtering
    - http://www.ietf.org/rfc/rfc2827.txt
- Hardening Information
  - Center for Internet Security
    - http://www.cisecurity.org/
  - Cisco SAFE
    - http://www.cisco.com/en/US/netsol/ns954/index.html
  - Country IP Blocks
    - http://www.countryipblocks.net/
  - DISA STIG's
    - http://iase.disa.mil/stigs/

Threats to your data never go away.
Neither should your security partner.
Making the unseen seen

Resources (cont'd)

Jacads
Strategic IT security solutions.

- Tools
  - Low Orbit Ion Cannon
    - http://sourceforge.net/projects/loic/
  - slowhttptest
    - http://code.google.com/p/slowhttptest/
  - Advanced Policy Firewall (APF)
    - http://www.rfxn.com/projects/advanced-policy-firewall/
  - (D)DoS Deflate
    - http://deflate.medialayer.com/
  - UrlScan
    - http://technet.microsoft.com/en-us/security/cc242650
  - Dynamic IP Restrictions
    - http://www.iis.net/download/DynamicIPRestrictions
- Apache Modules
  - Mod_evasive
    - http://www.topwebhosts.org/articles/mod_evasive.php
  - Mod_security
    - http://www.topwebhosts.org/articles/mod_security.php

Follow-up

Jacadis
Strategic IT security solutions.

jbrennen@jacadis.com

https://about.me/slandail

Any questions?

Threats to your data never go away.
Neither should your security partner.
Making the unseen seen