Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Denial of Service

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Understanding DoS

- The aim is to disrupt communication with important resources
- This affects the Availability in the CIA triad
- Unavailability of resources
- Loss of access to a website
- Slow performance
- Increase in spam emails
- Can result in the loss of millions of dollars
  - Websites that rely on traffic for income cannot earn money

DoS Targets

- Web server compromise – loss of uptime
- Back-end resources – take down means all frontend becomes useless
- Network or Computer Specific

Types of Attacks

- Service Request Floods
- SYN Attack/Flood
- ICMP Flood Attack
- Ping of Death
- Teardrop
- Smurf
- Fraggle
- Land

Permanent DoS Attack

- Phlashing is a form of permanent DoS that pushes bogus updates to the victim's firmware. The hardware becomes unusable.
- This is how you "brick" a device

Application Level Attacks

- **Flood**
  - **Overwhelm the target with traffic making it difficult to send a response**
- **Disrupt**
  - **An example would be attempting to login as a user several times so it locks them out of their account**
- **Jam**
  - **Specially crafted queries can lock up a database**

Understanding DDoS

- **DDoS Attacks**
  - **Distributed Denial of Service**
  - **Several attackers are attacking the same target**
  - **“Bot” – infects the handler or master computer**
  - **“slaves” or “zombies” – clients used by the master server bot**
  - **Multiple handlers can control multiple zombies in a huge distributed tree**

DoS Tools

- DoSHTTP
- UDPFlood
- Jolt2
- Targa

DDoS Tools

- Trinoo
- Low Orbit Ion Cannon
- TFN2K
- Stacheldraht

DoS Defense Strategies

- Disable unnecessary services
- Use Anti-virus
- Enable Router Throttling
- Use a Reverse Proxy
- Enable Ingress and Egress Filtering
- Degrading Services
- Absorbing the Attack

Botnet-Specific Defenses

- RFC 3704 Filtering
- Black Hole Filtering
- Source IP Reputation Filtering

Conclusion

- Understand the Targets
- Know the Stack
- Understand buffer overflow
- Know the dangerous C functions
- Understand the NOP sled
- Be familiar with attack methods
- Know the prevention
- Know tools and terms