ASLR: How Robust is the Randomness?

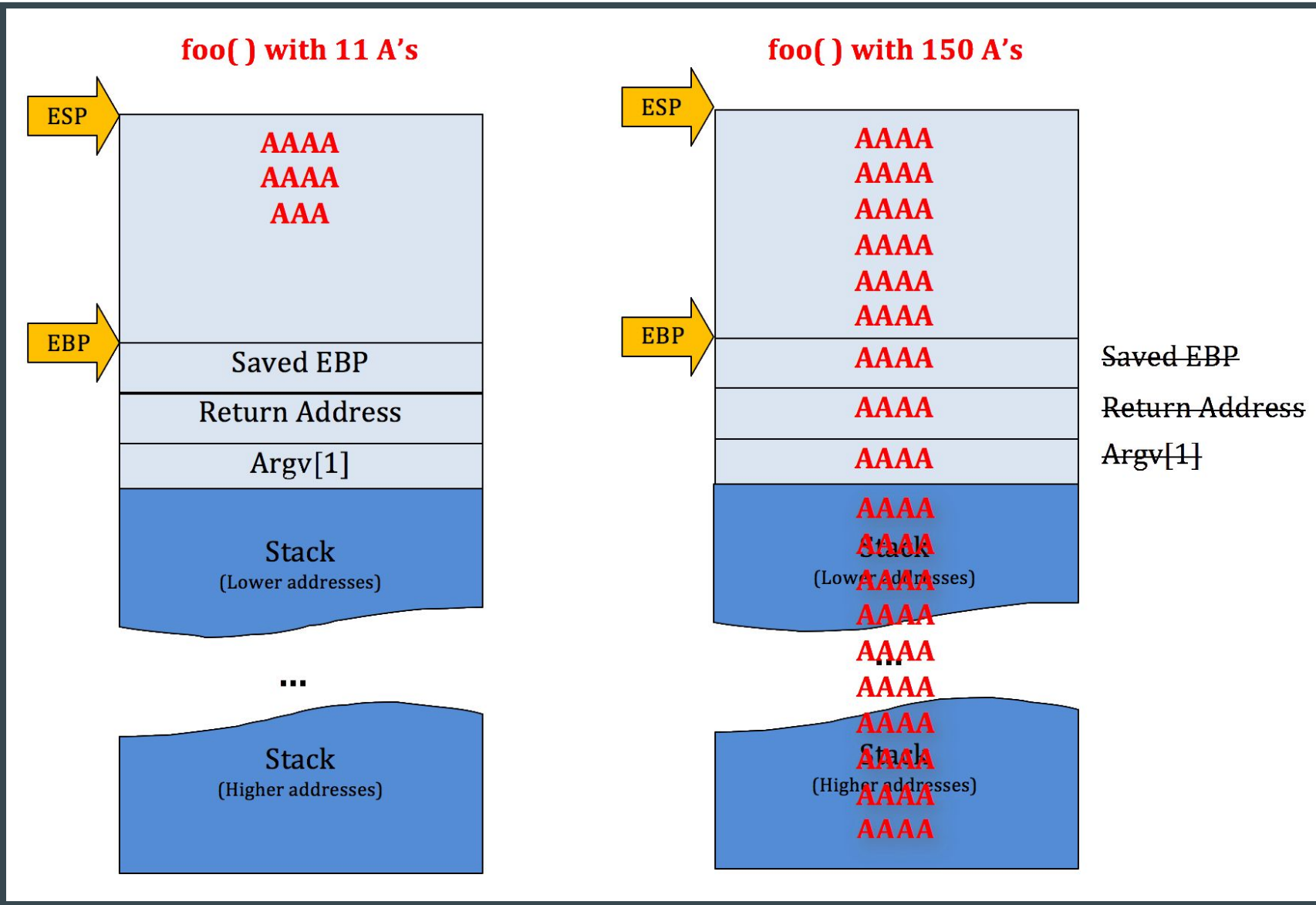
...

Jonathan Ganz

What is Address Space Layout Randomization?

- Provides System-Level Control-Flow Integrity
- Adds Random Memory Offsets to Binaries
- Makes Buffer Overflows Harder to Exploit
  - Does Not Completely Remove Vulnerability
- Strength of ASLR Depends on Entropy of Offsets

What are Buffer Overflows?



https://www.securitysift.com/windows-exploit-development-part-2-intro-stack-overflow/

Why Attackers Perform Buffer Overflows

Why We Use ASLR

- Organizations Often Rely on Third-Party Software
- This Software May Be Vulnerable & Closed-Source
- Extra Hardening Features May Not Be Available
  - CPU Power
  - Thermal Design Power
  - Licensing / Cost
  - Architecture Compatibility

Motivation

- We Rely on Certain Security Features
- How Reliable are these Features?
- How Much Defense Does ASLR Provide?
- Remote Security Evaluation

ASLR Experiment

- Measure Entropy of ASLR Implementations
- Develop Buffer-Overflow-Vulnerable Program
- Develop Attack Program (Inspired by Blind-ROP)
- Evaluate Multiple Operating Systems
  - Debian, OpenBSD, HardenedBSD
  - 32-bit and 64-bit Architectures
- Perform Hundreds of Measurements

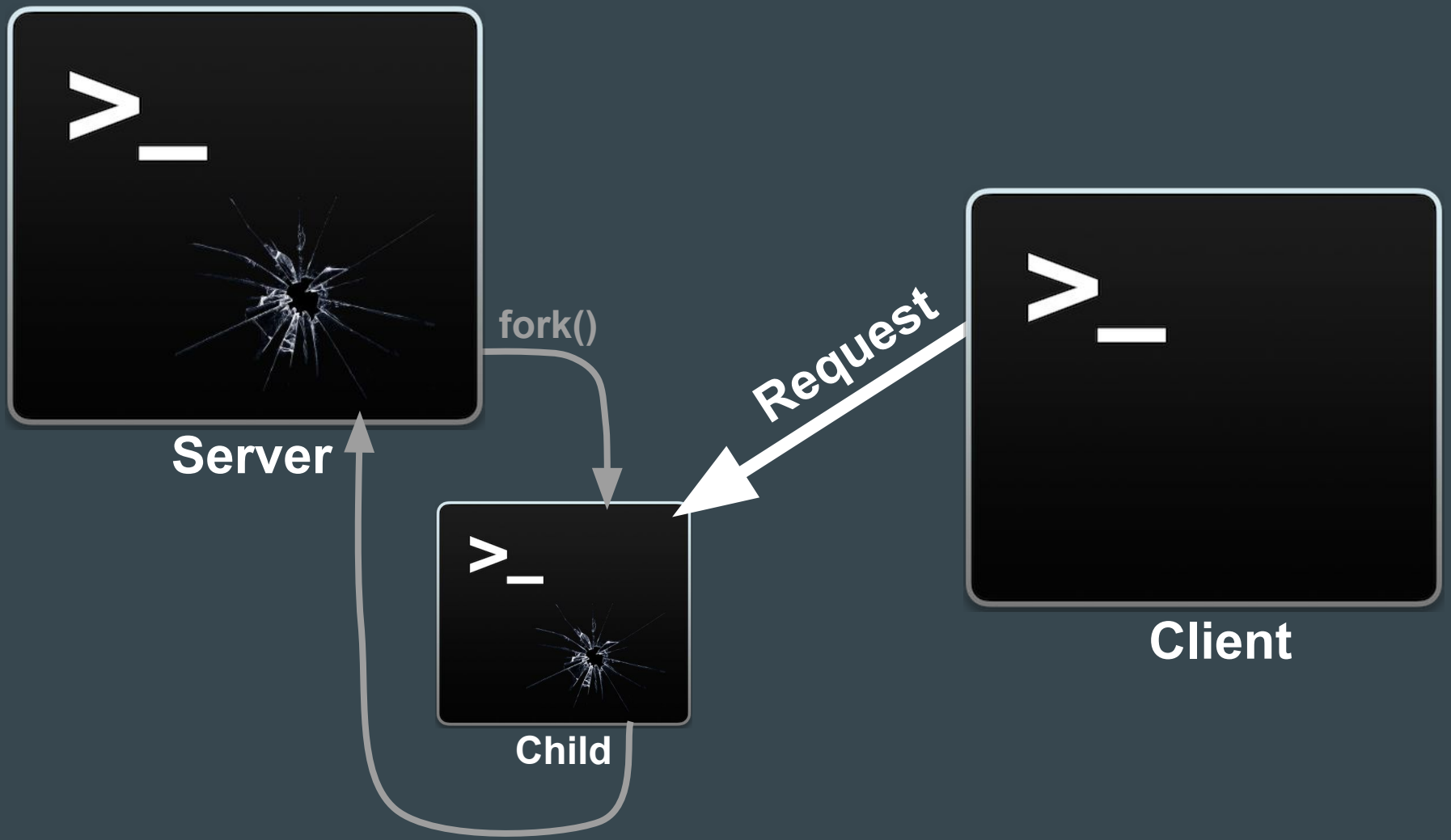
ASLR Assumption

- 64-bit Operating Systems Represent Memory with More Bits than their 32-bit Variants
- The 64-bit Versions Have More Bits Available to Manipulate Through ASLR
- 64-bit Implementations of ASLR Should Provide More Entropy than 32-bit Implementations

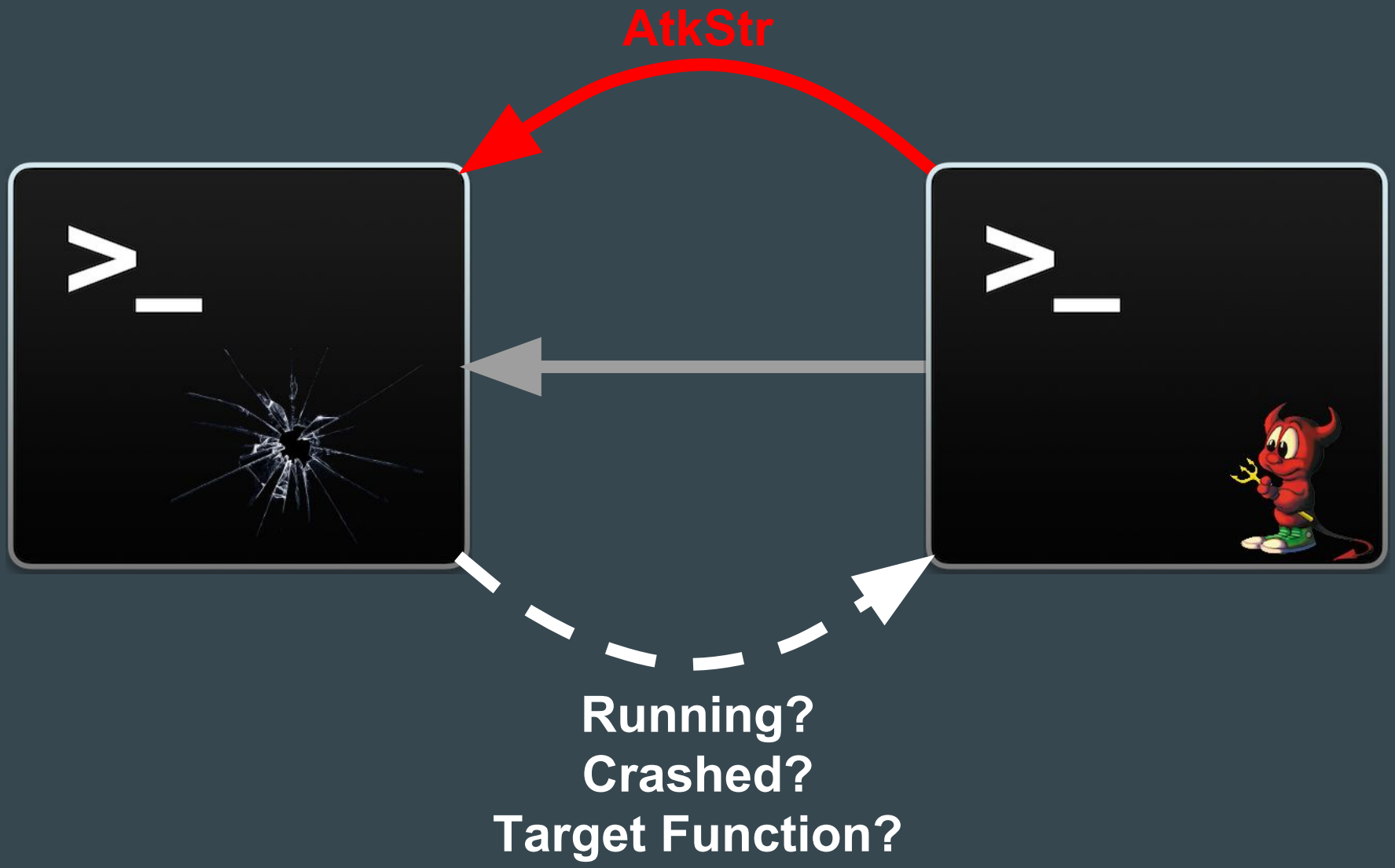
Claims of Entropy Provided by ASLR

	Entropy Claimed
64-bit HardenedBSD	30 bits
64-bit Debian	28 bits
64-bit OpenBSD	25 bits
32-bit Debian	24 bits
32-bit OpenBSD	16 bits
32-bit HardenedBSD	14 bits

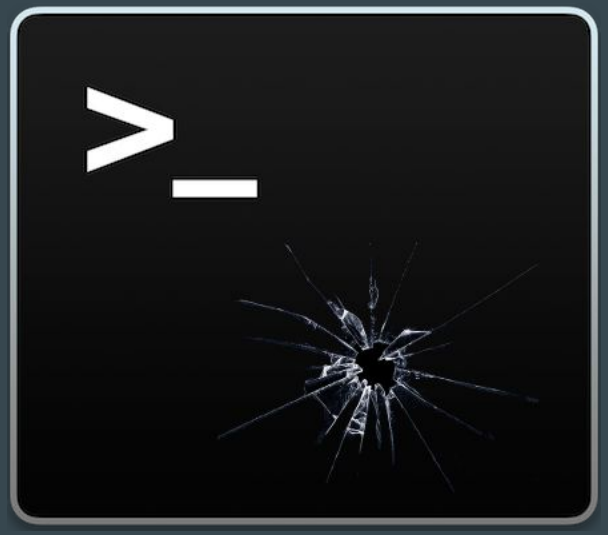
Vulnerable Network Service



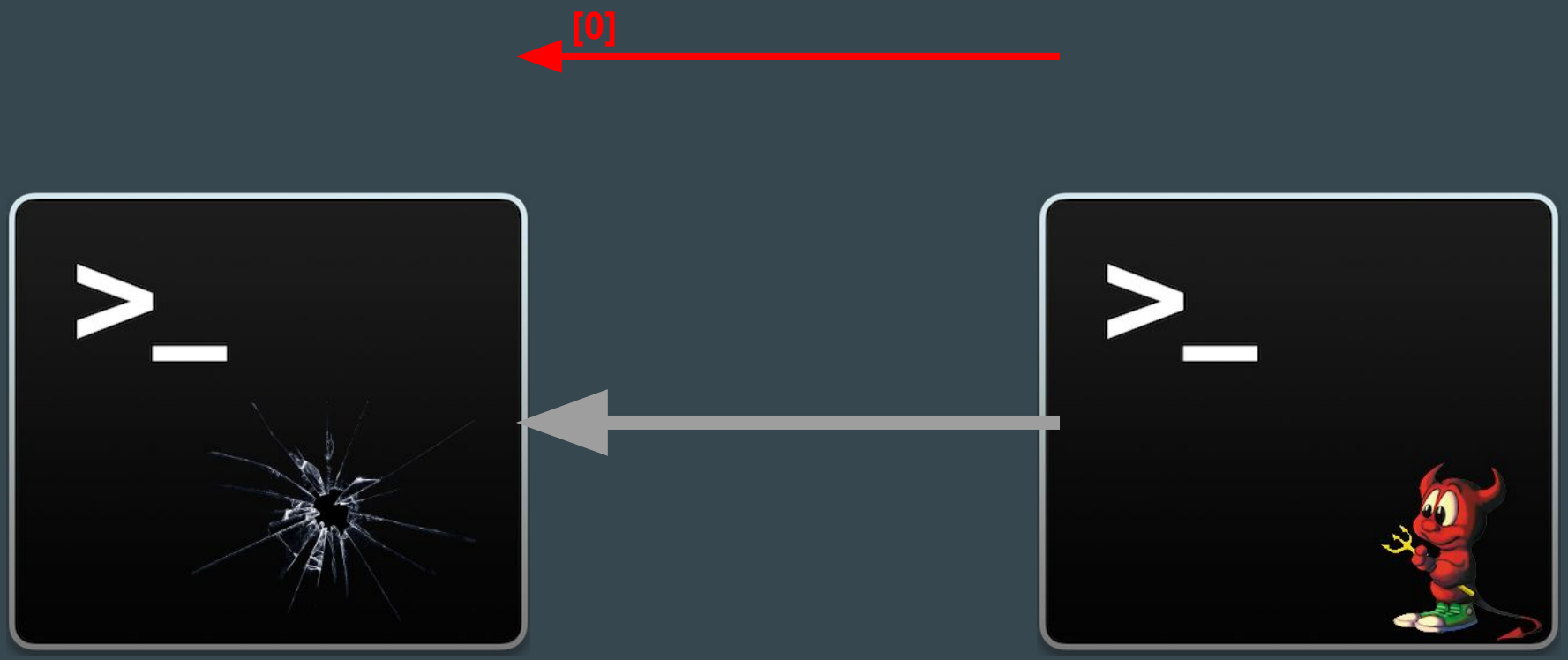
Attacking the Vulnerable Service



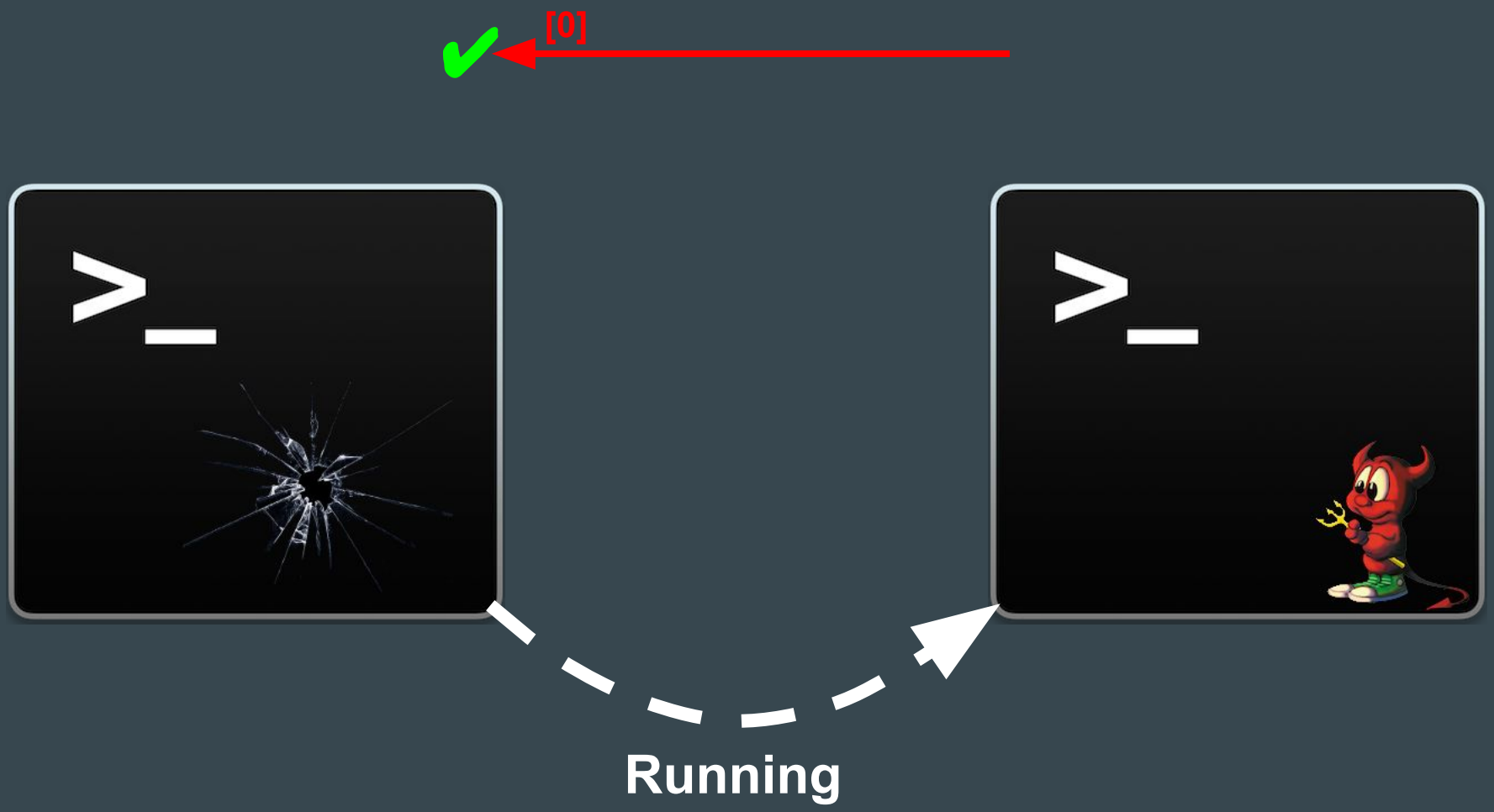
Attack Strategy



Attack Strategy

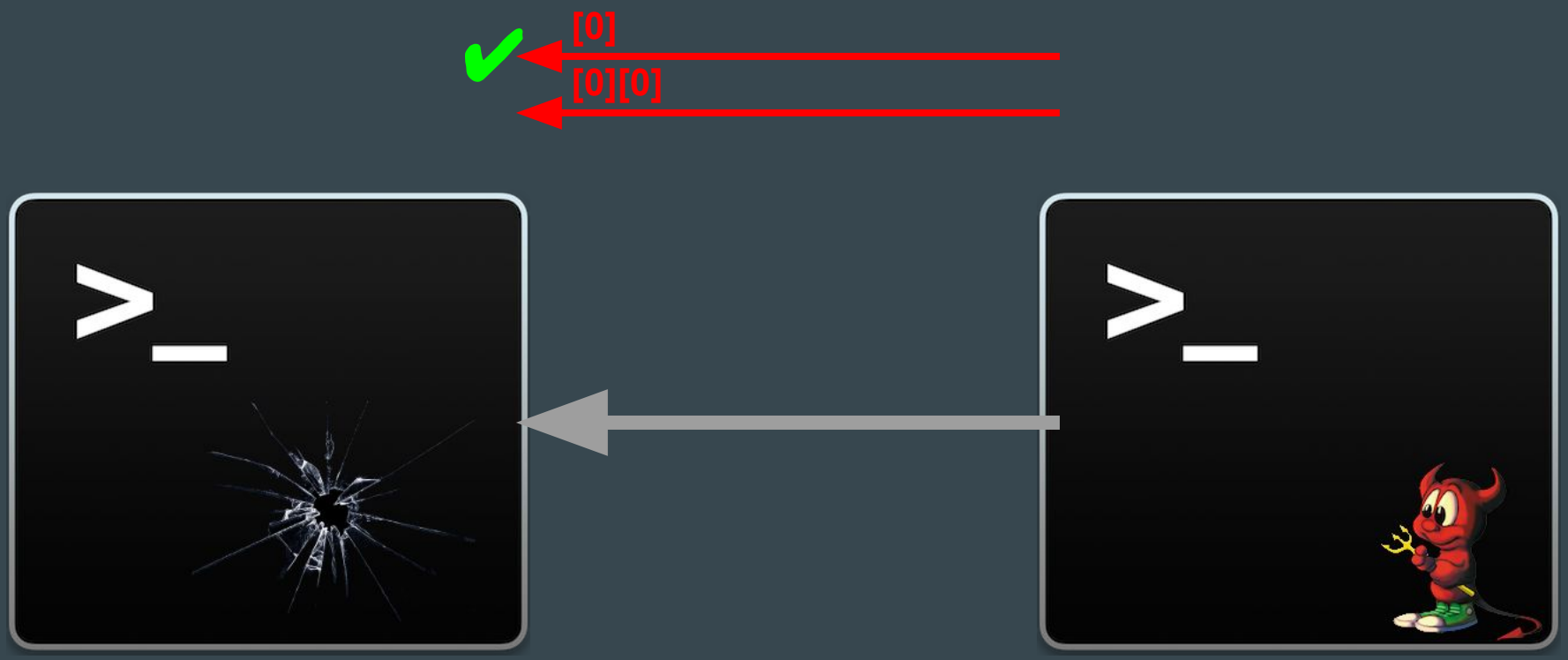


Attack Strategy

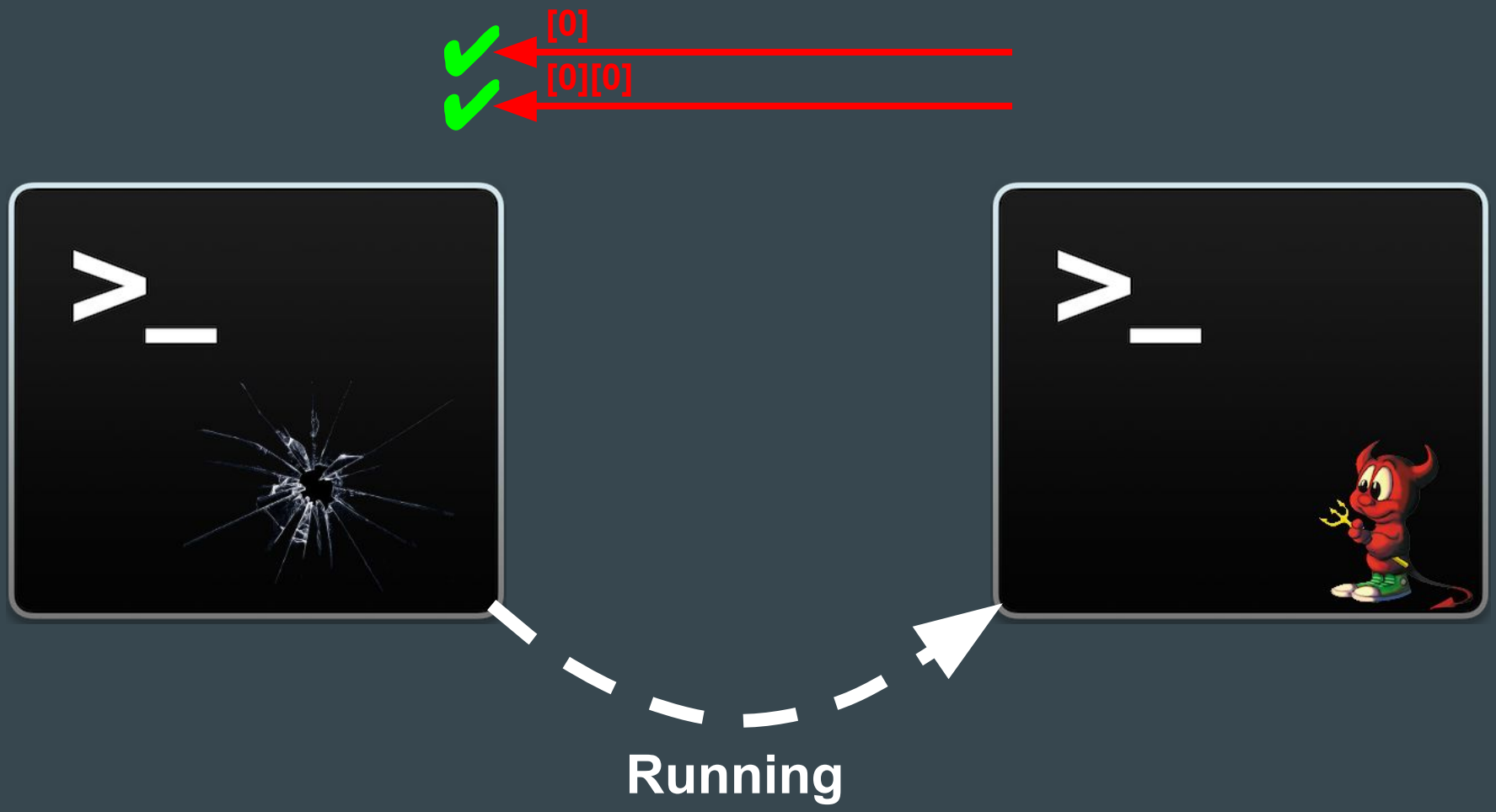


Attack Strategy

Attack Strategy

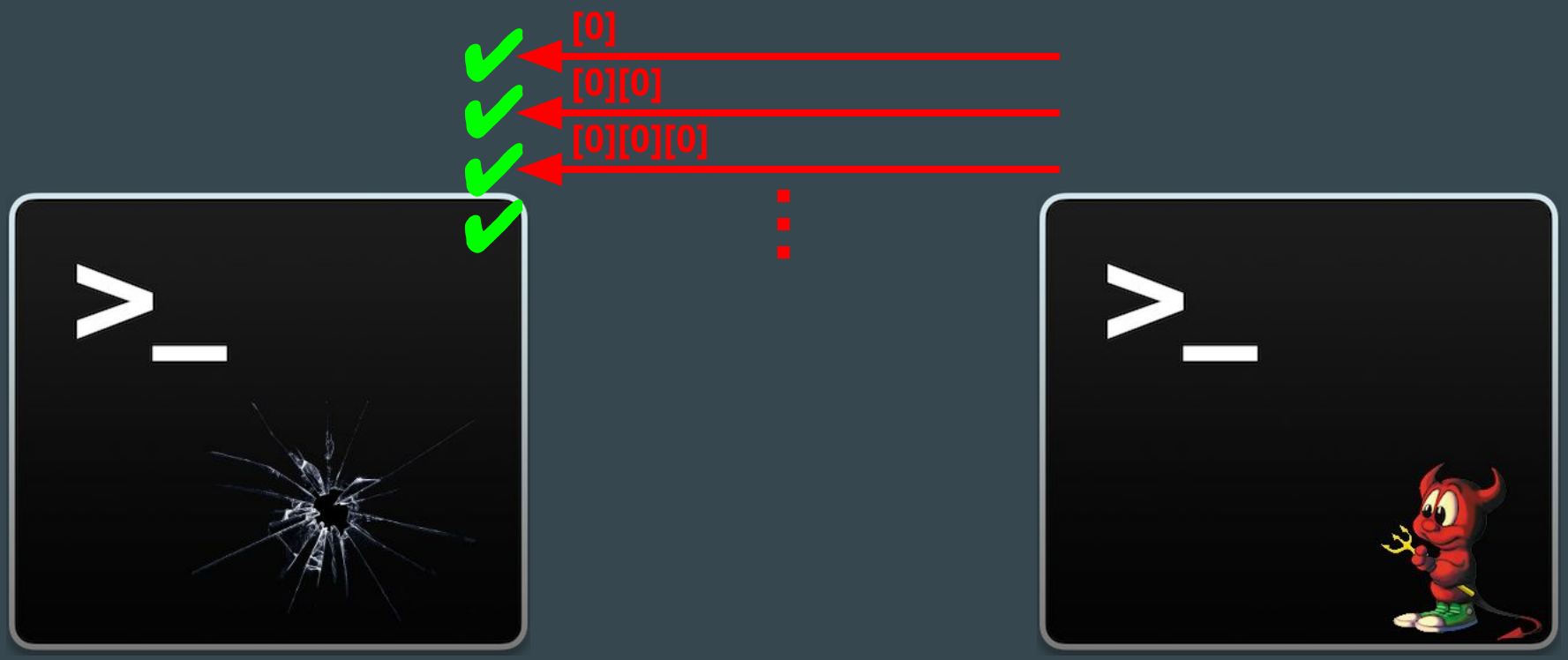


Attack Strategy

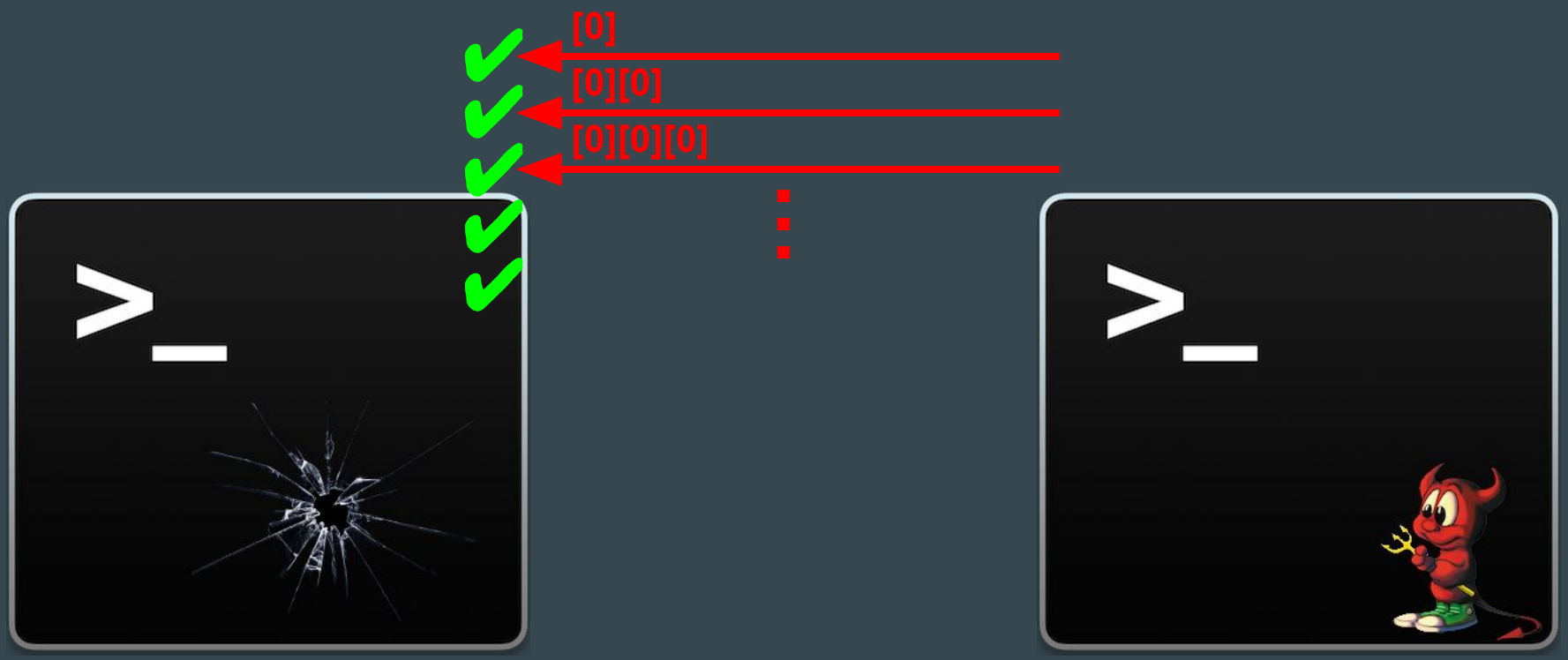


Attack Strategy

Attack Strategy

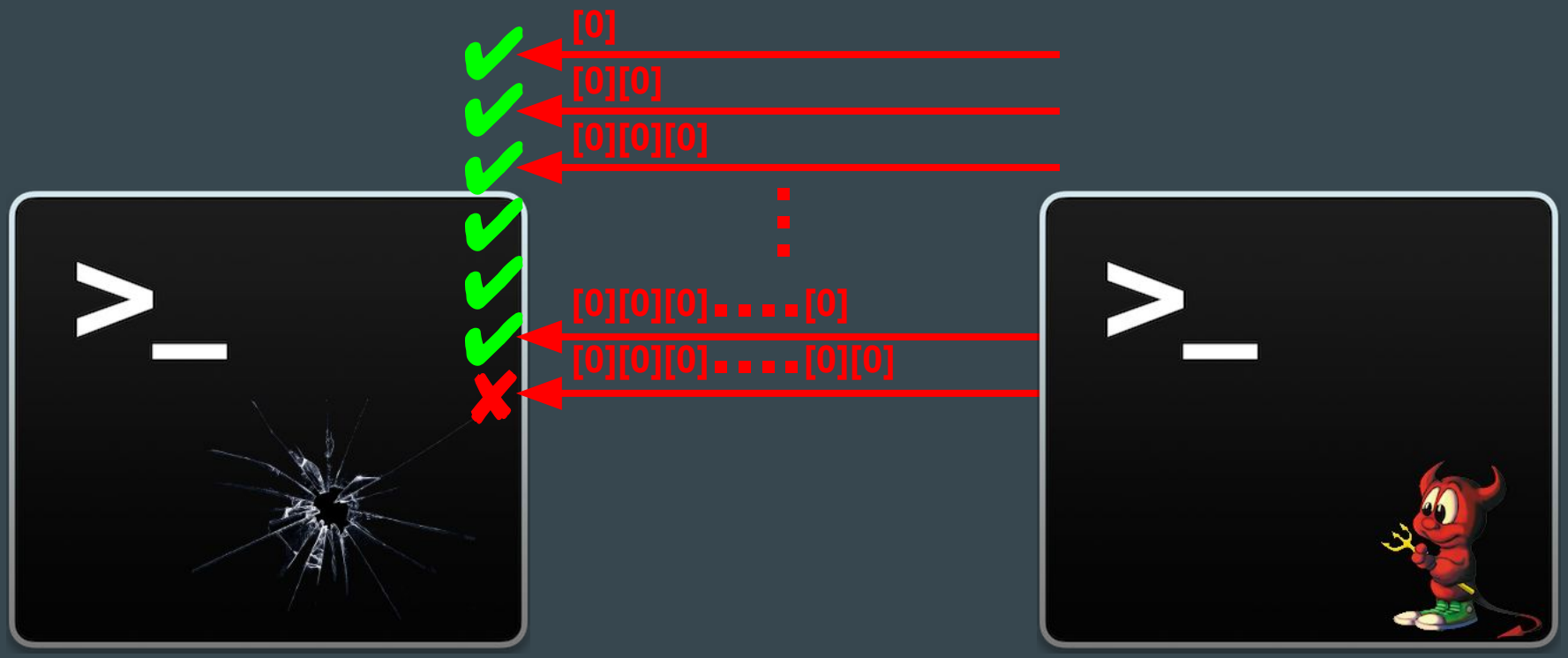


Attack Strategy

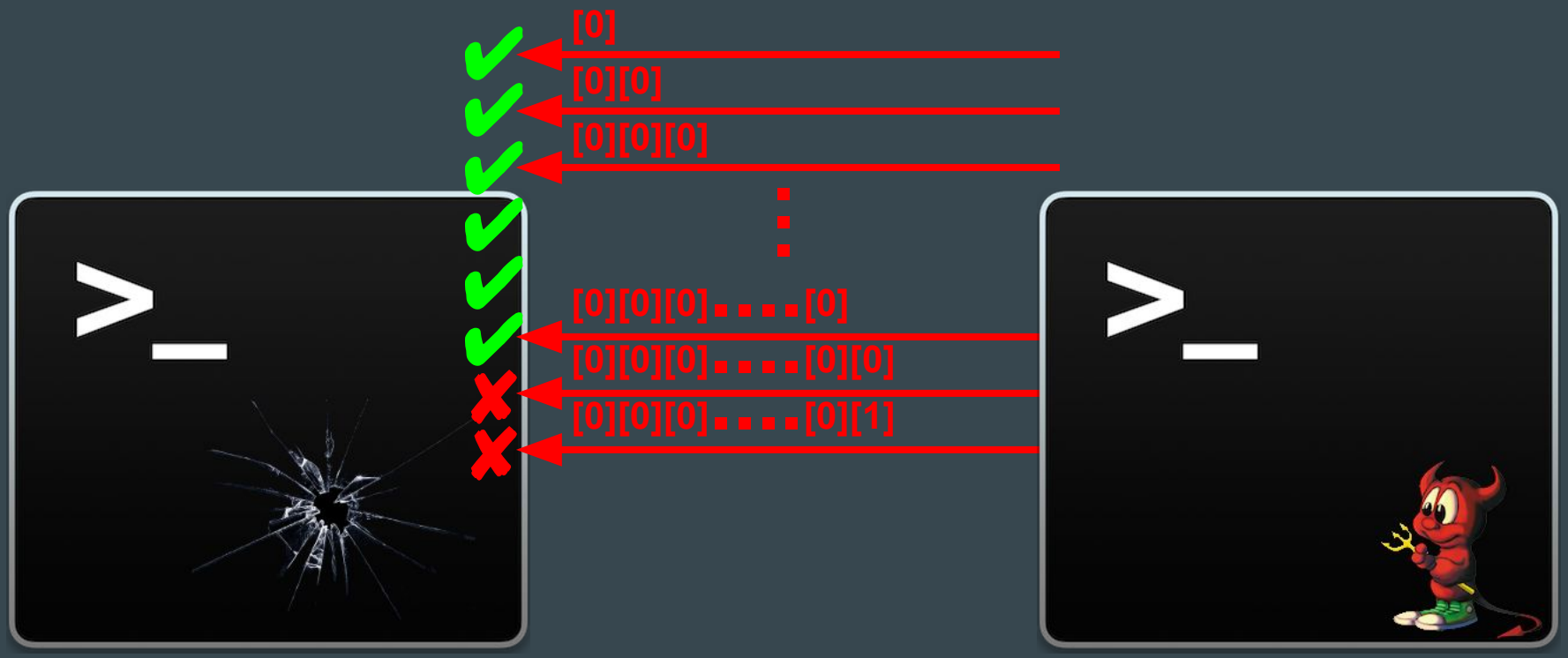


Attack Strategy

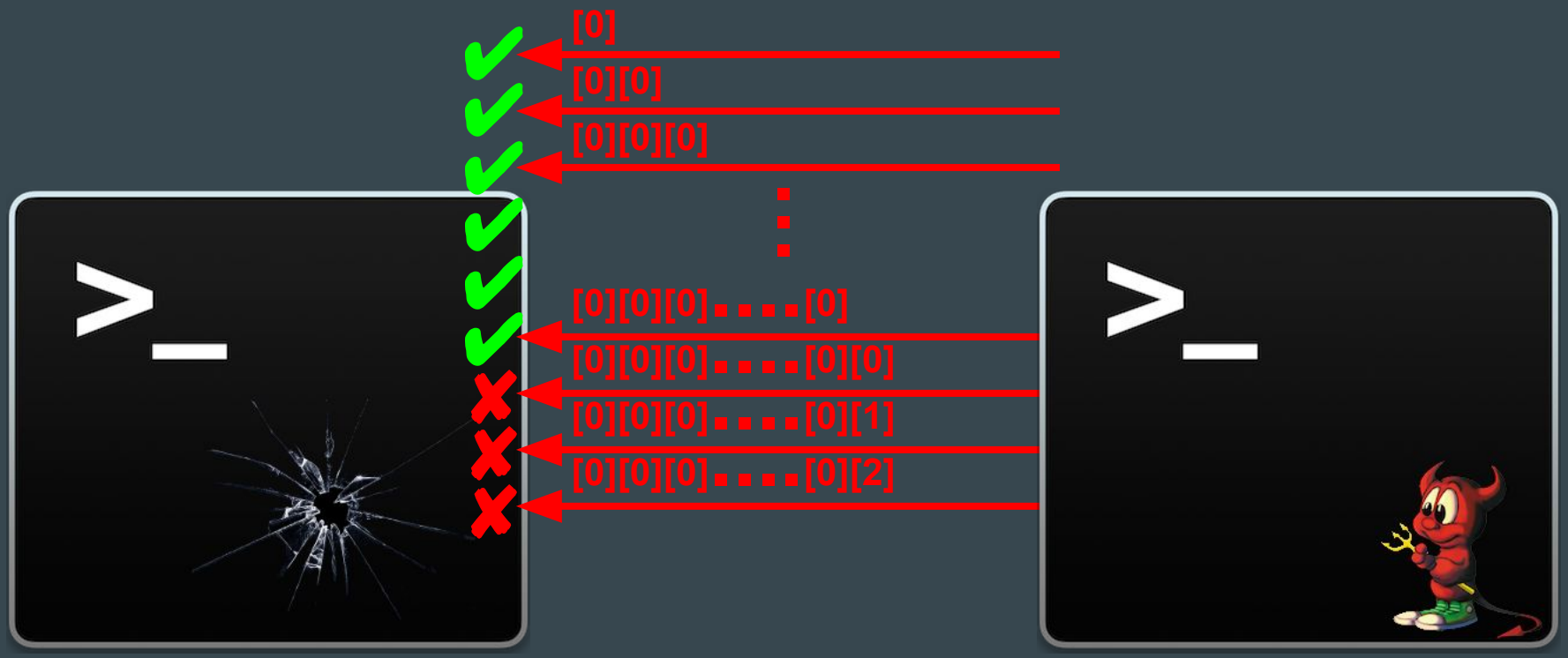
Attack Strategy



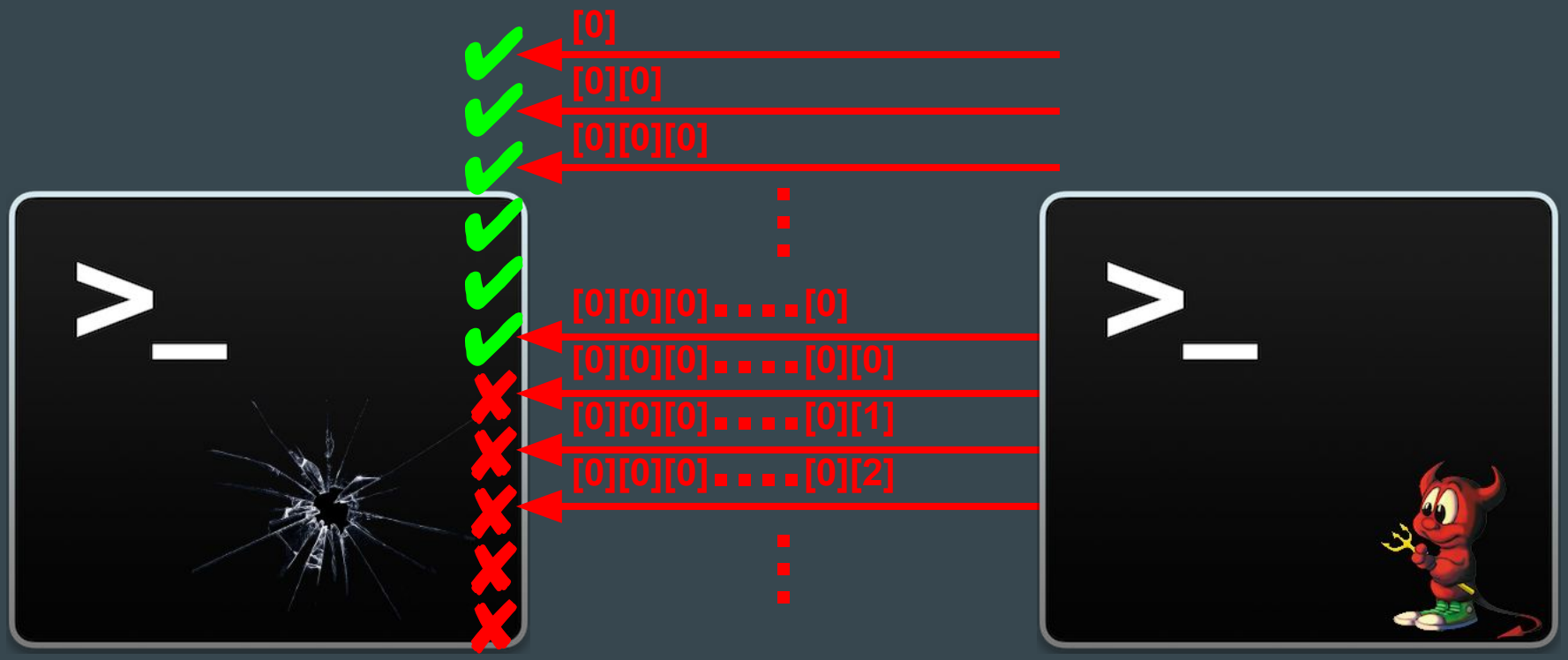
Attack Strategy



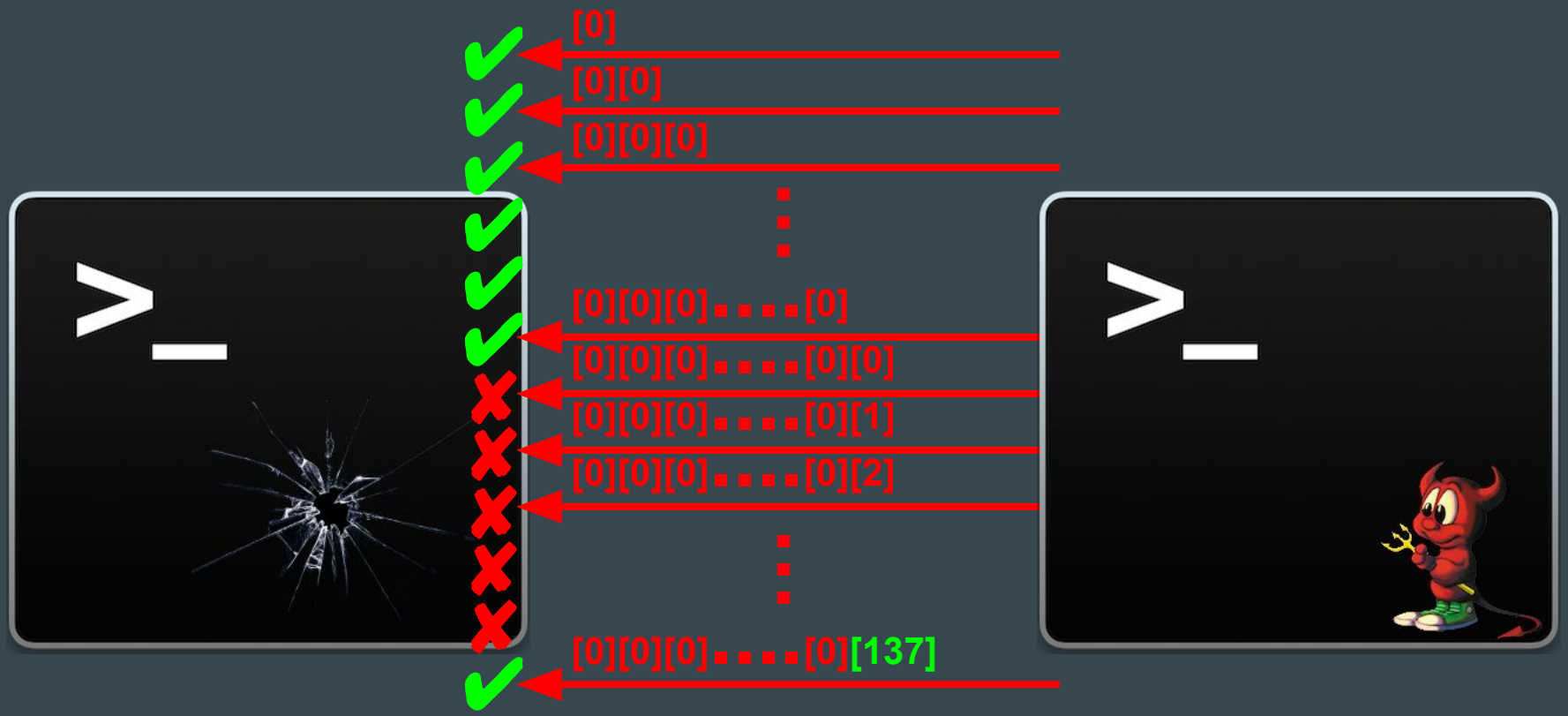
Attack Strategy



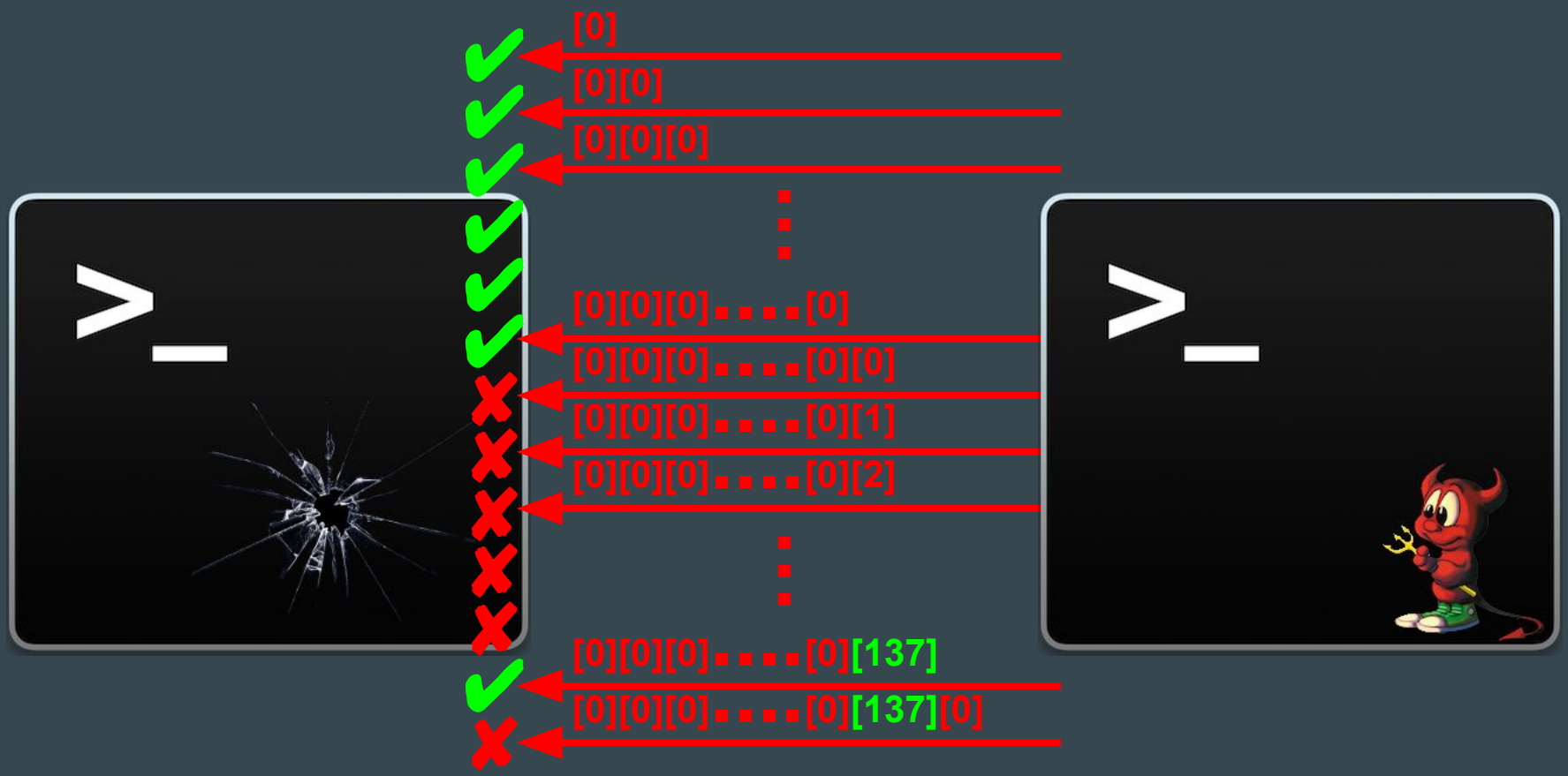
Attack Strategy



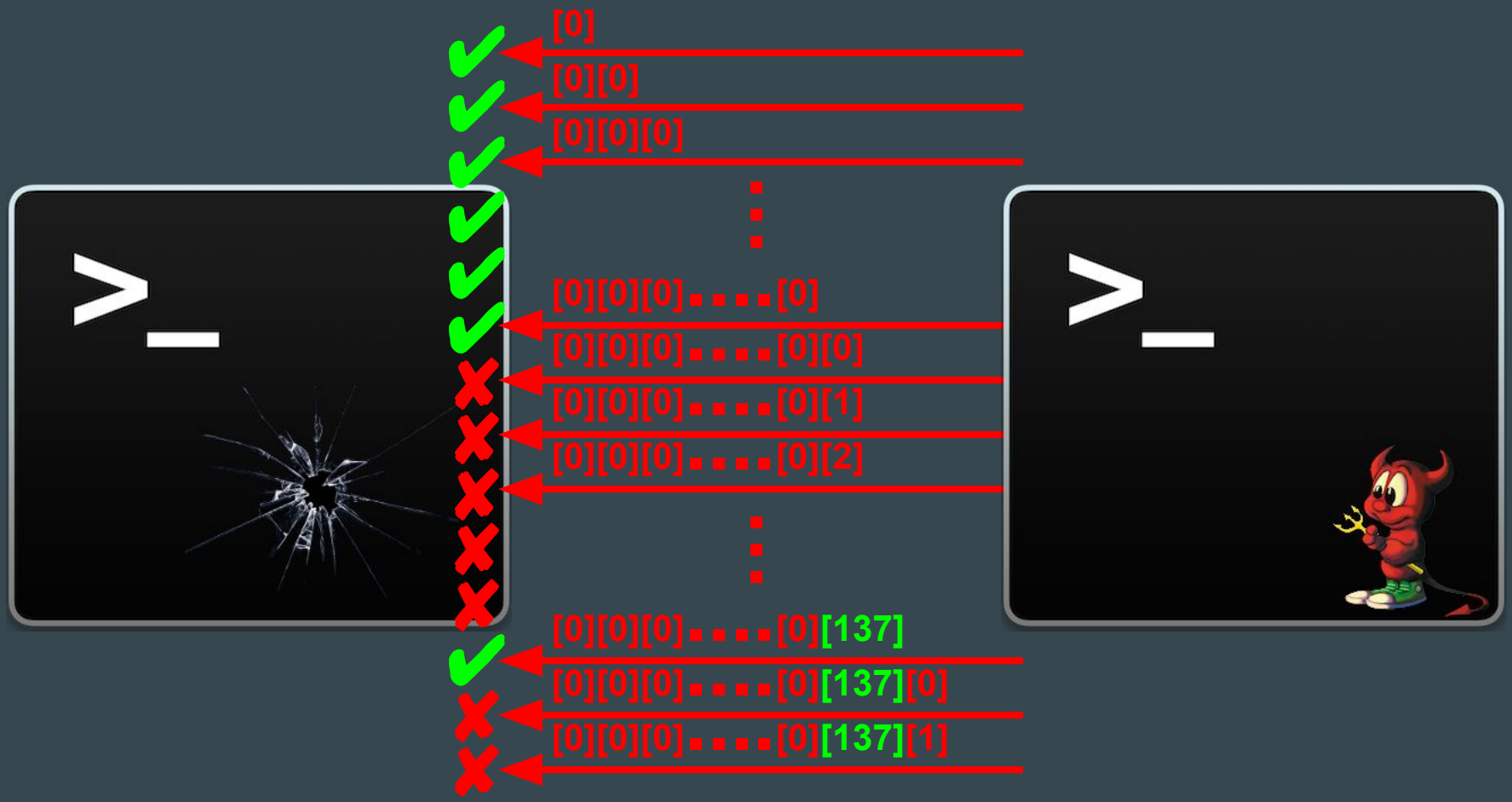
Attack Strategy



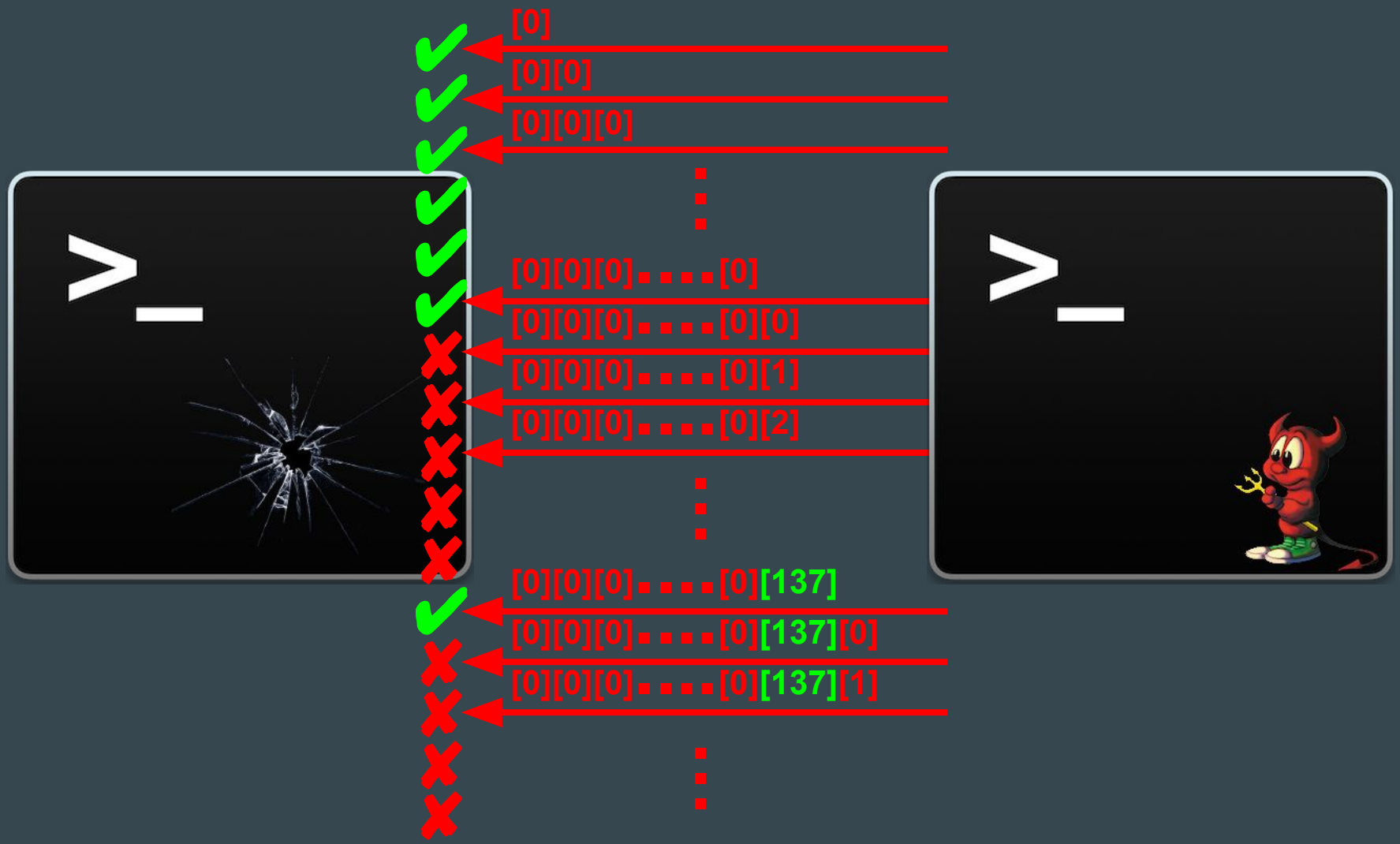
Attack Strategy



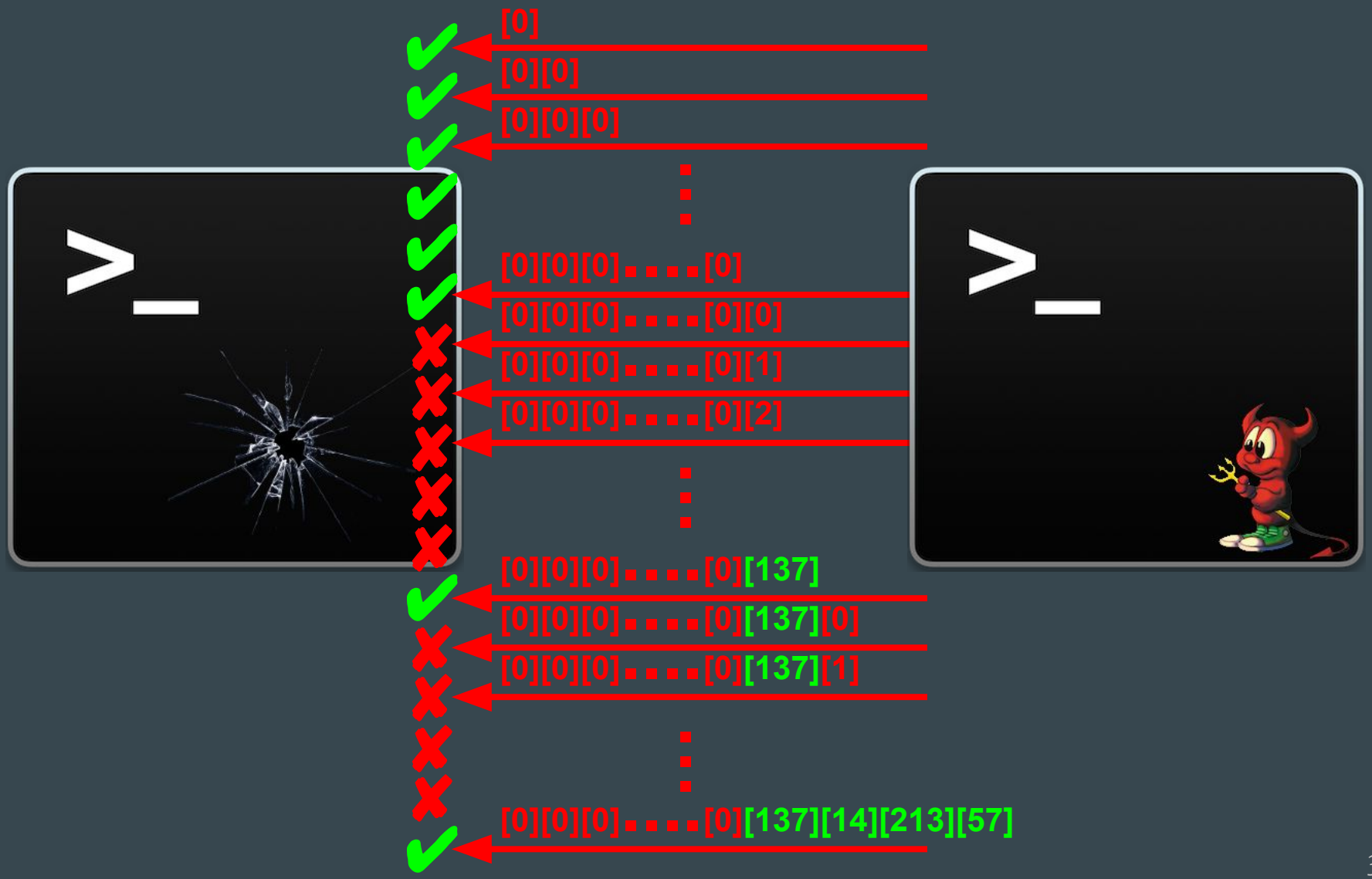
Attack Strategy



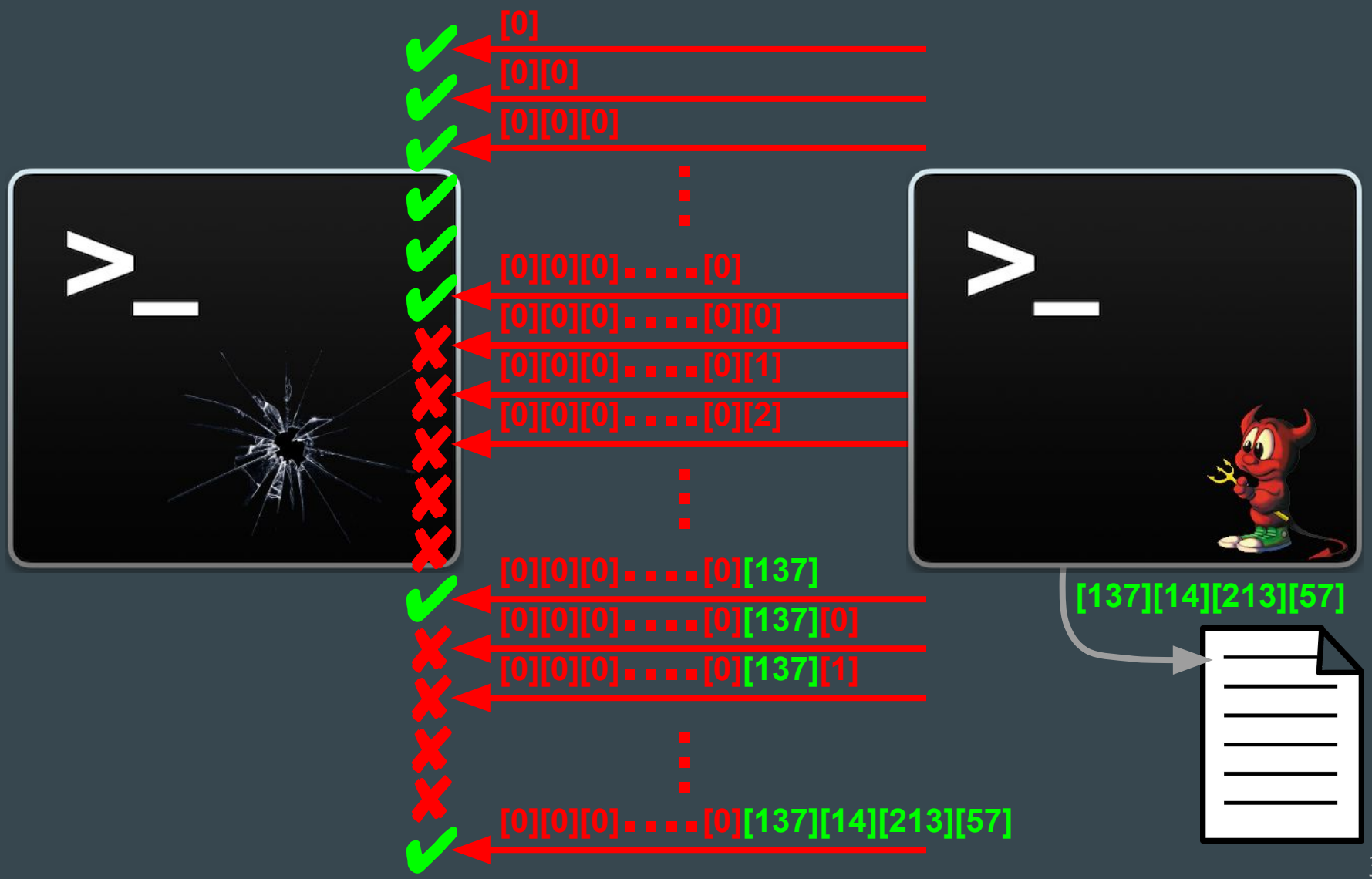
Attack Strategy



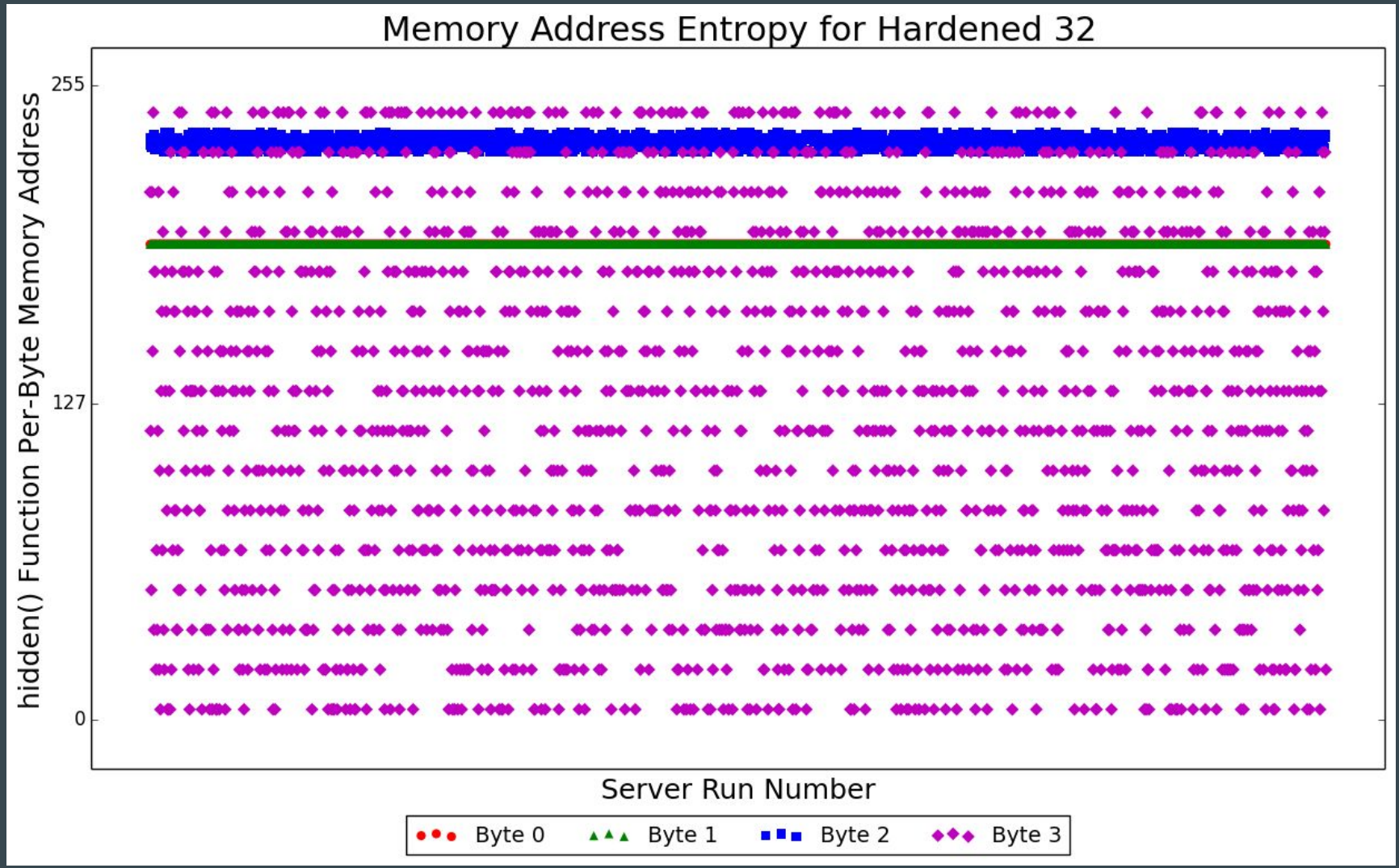
Attack Strategy



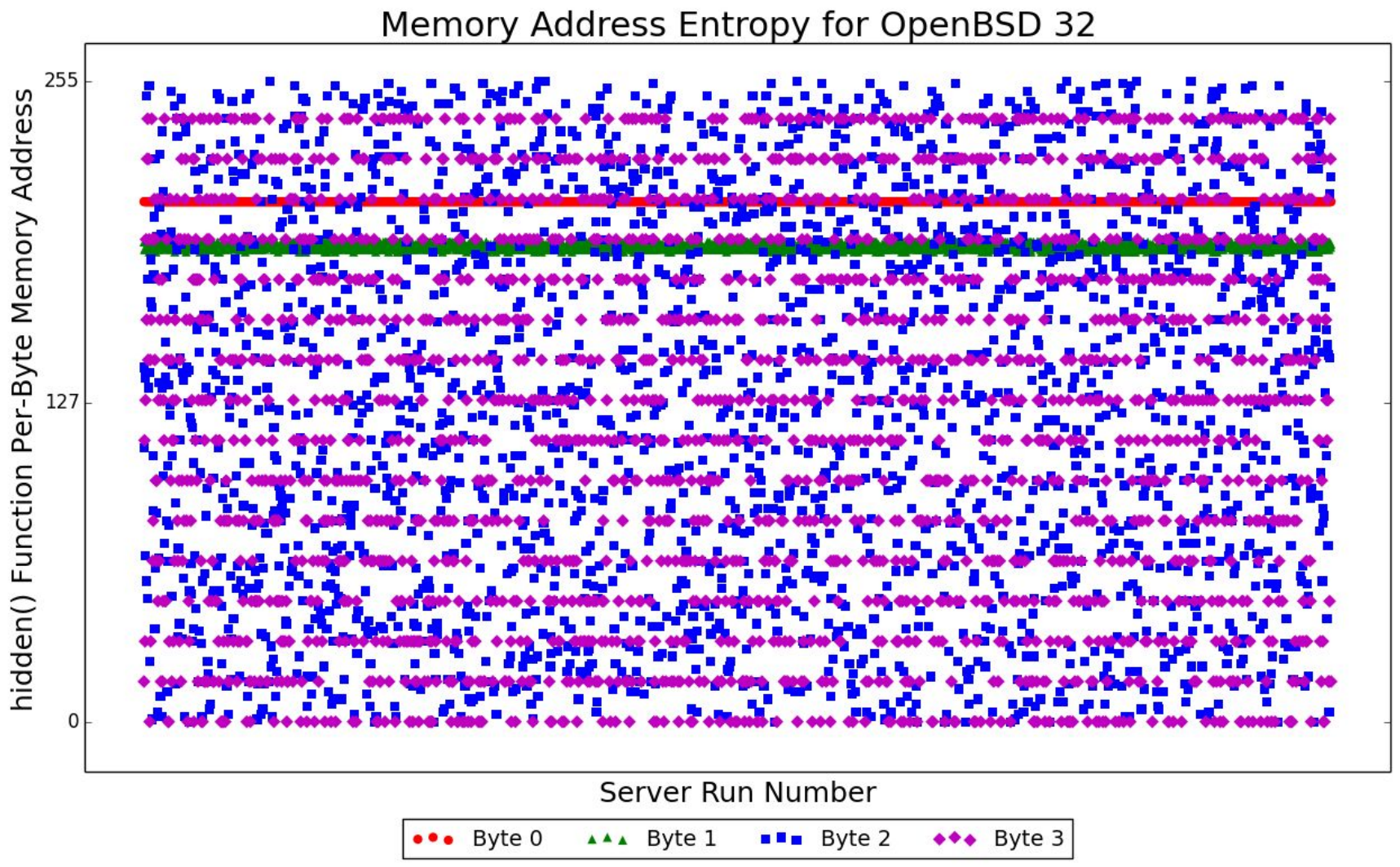
Attack Strategy



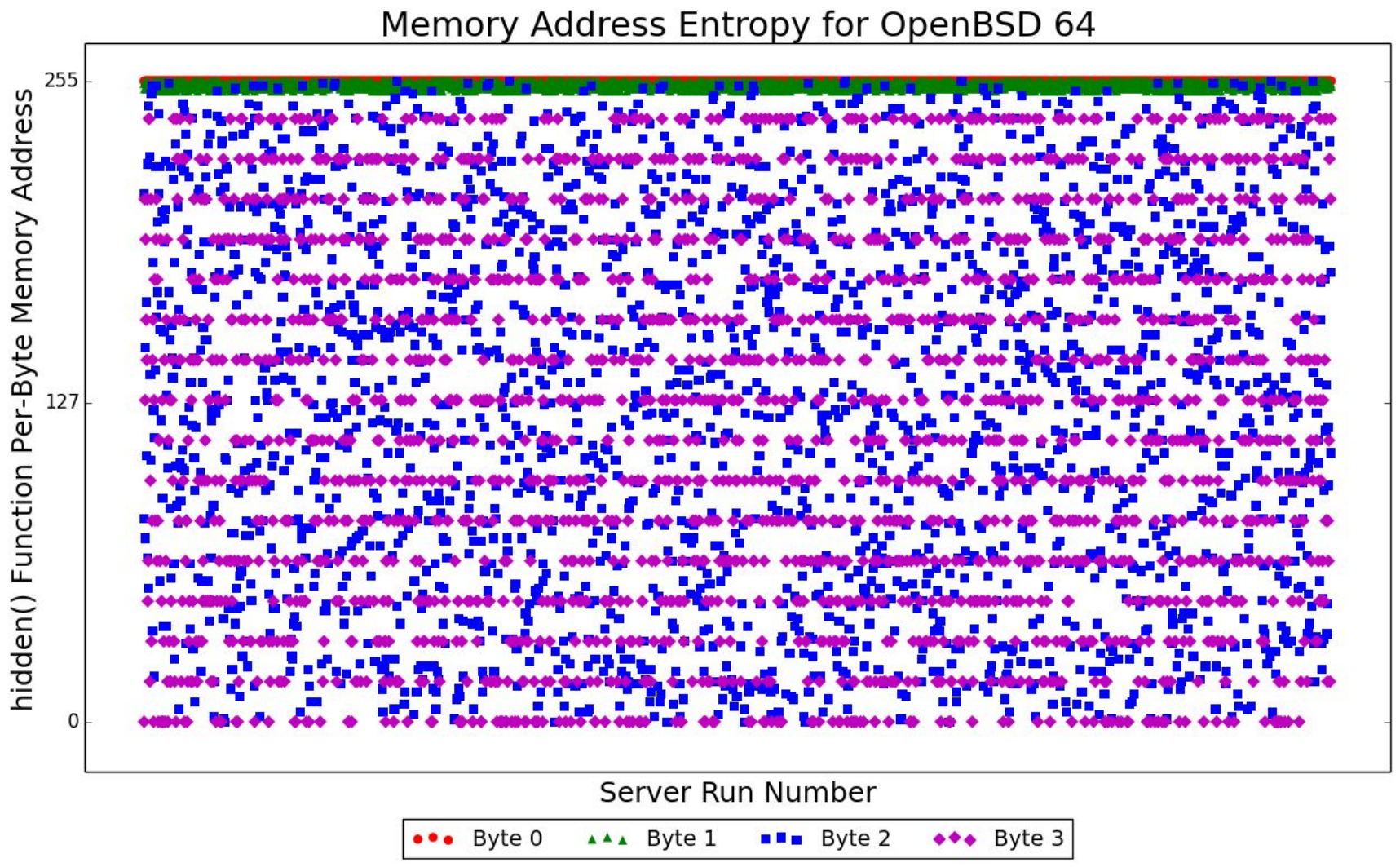
ASLR Results - 32-bit HardenedBSD



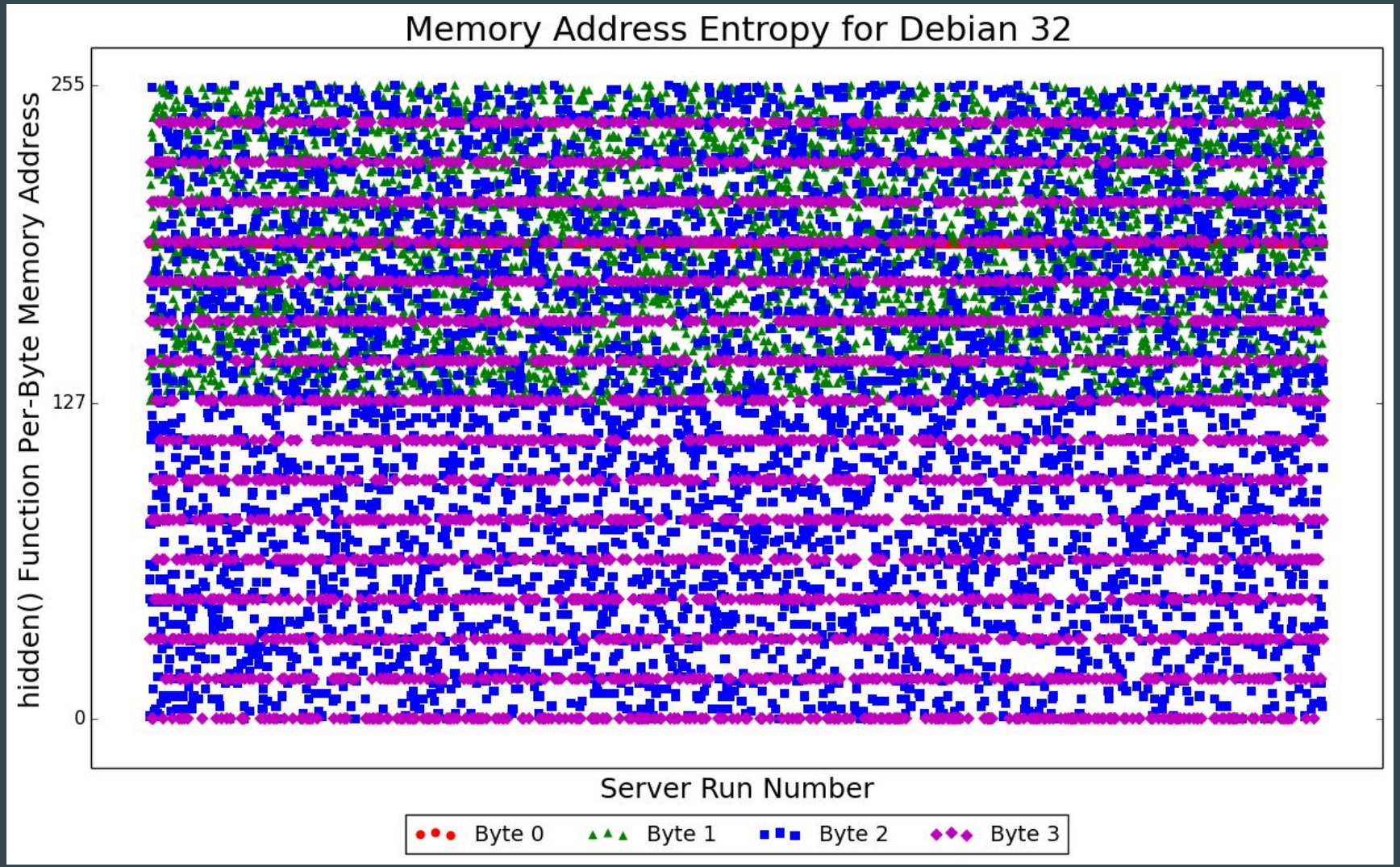
ASLR Results - 32-bit OpenBSD



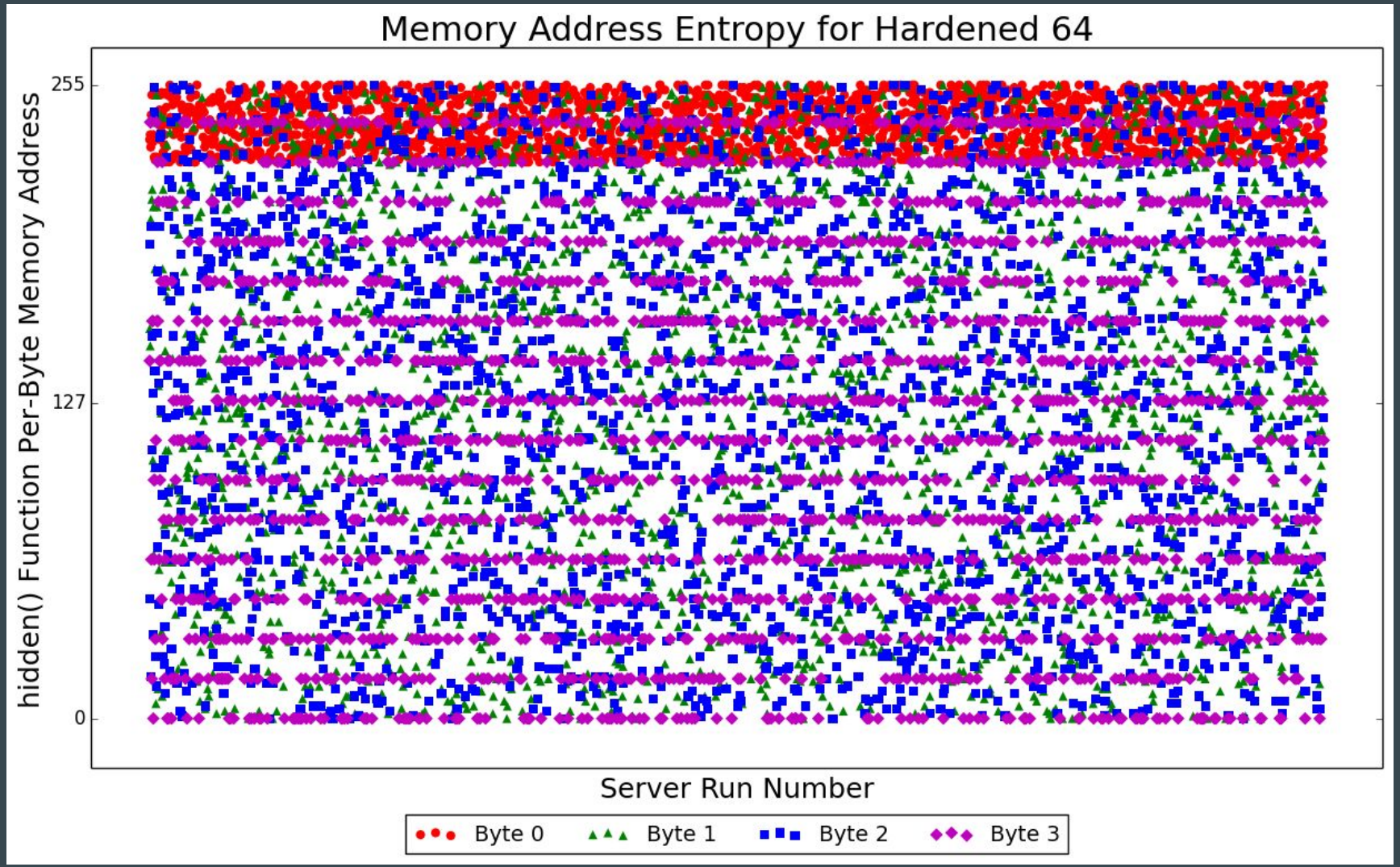
ASLR Results - 64-bit OpenBSD



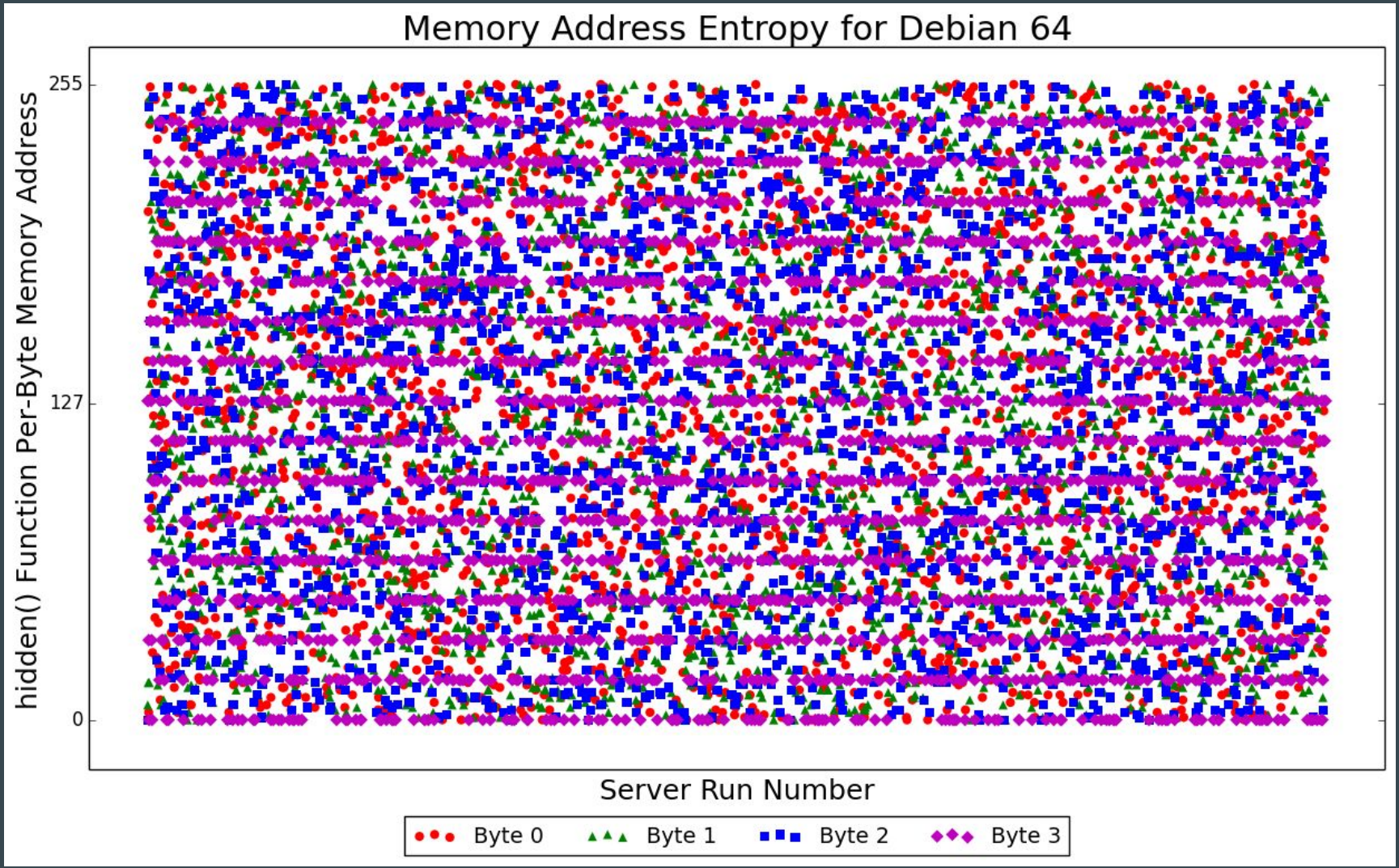
ASLR Results - 32-bit Debian Linux



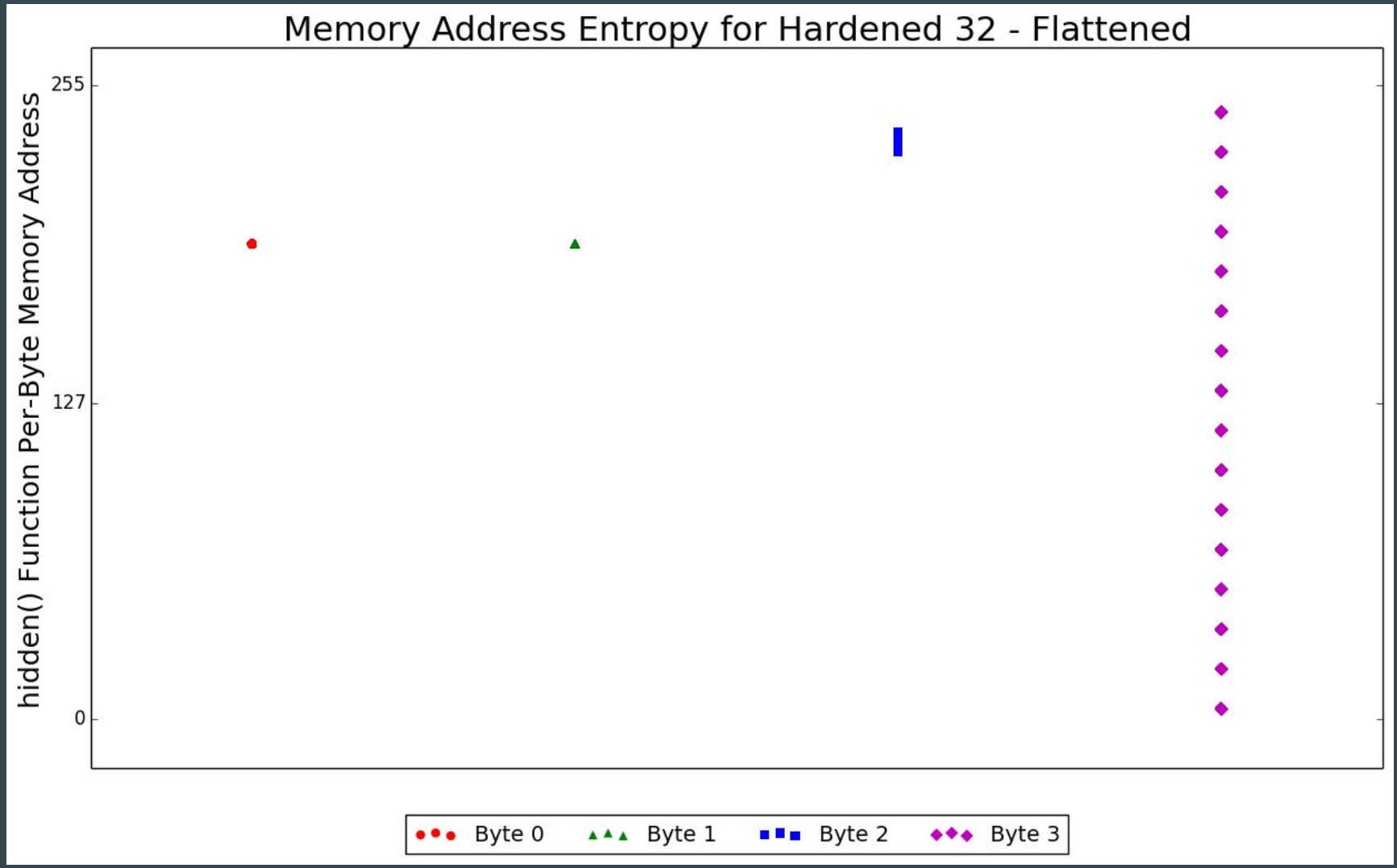
ASLR Results - 64-bit HardenedBSD



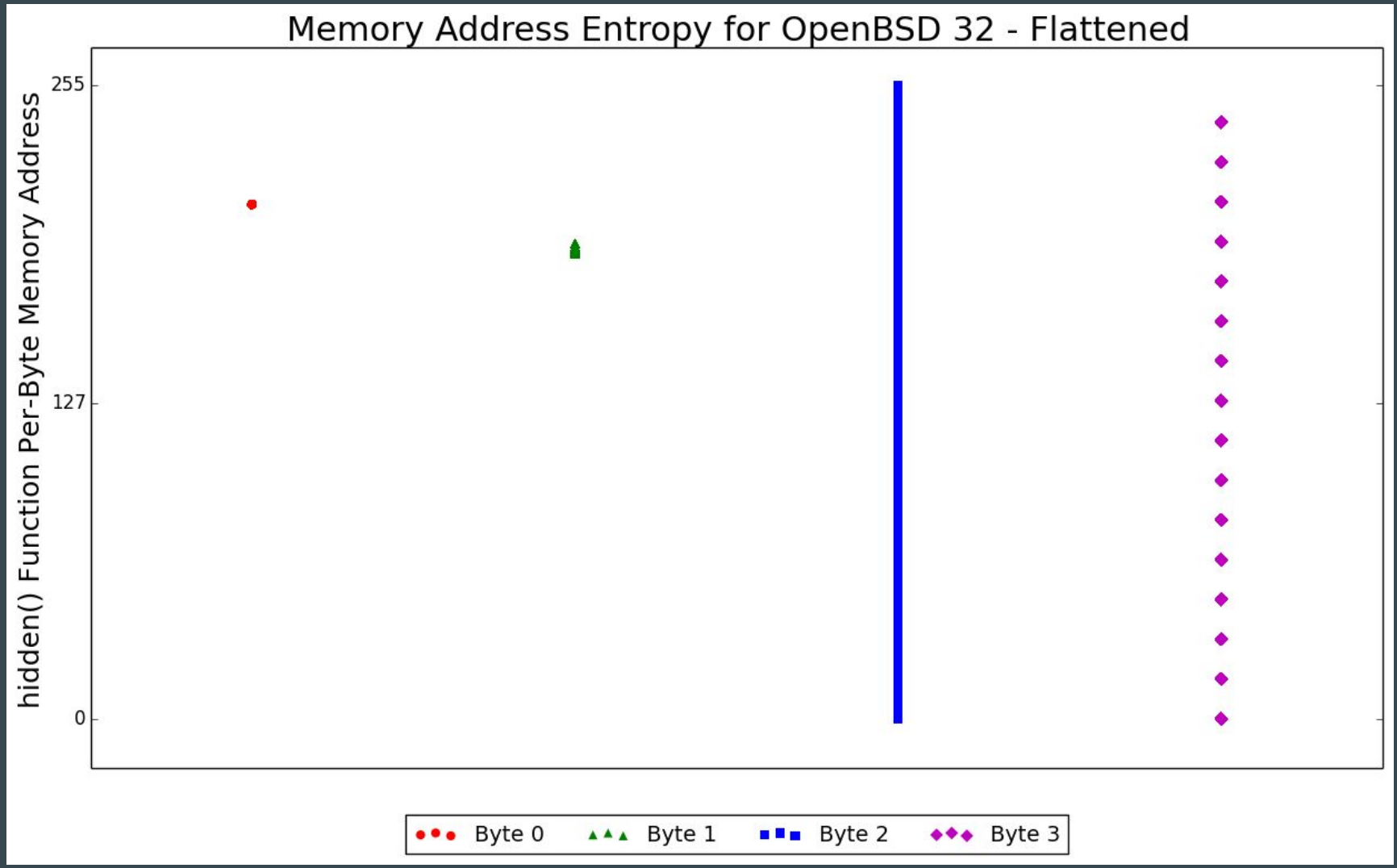
ASLR Results - 64-bit Debian Linux



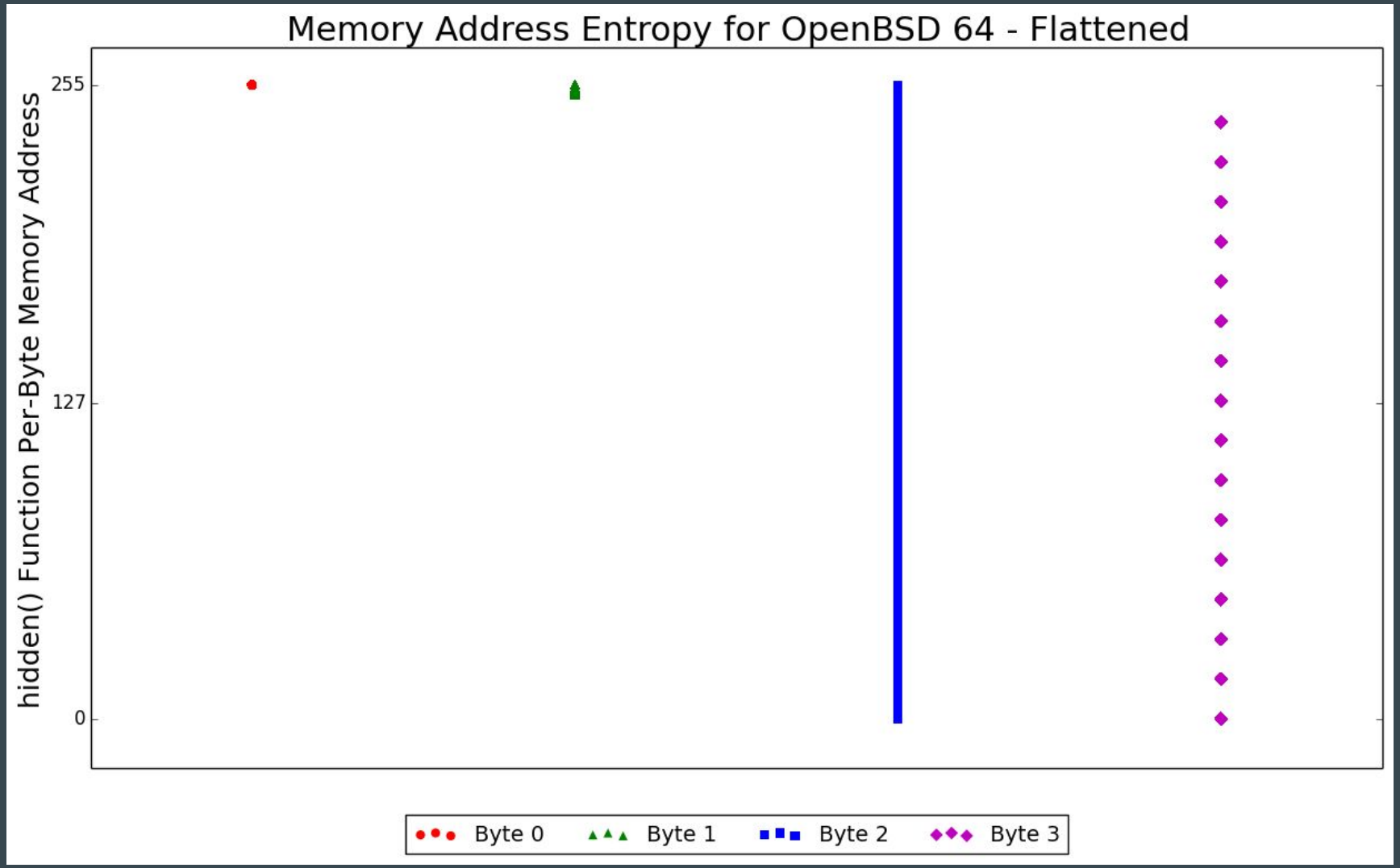
ASLR Results - 32-bit HardenedBSD



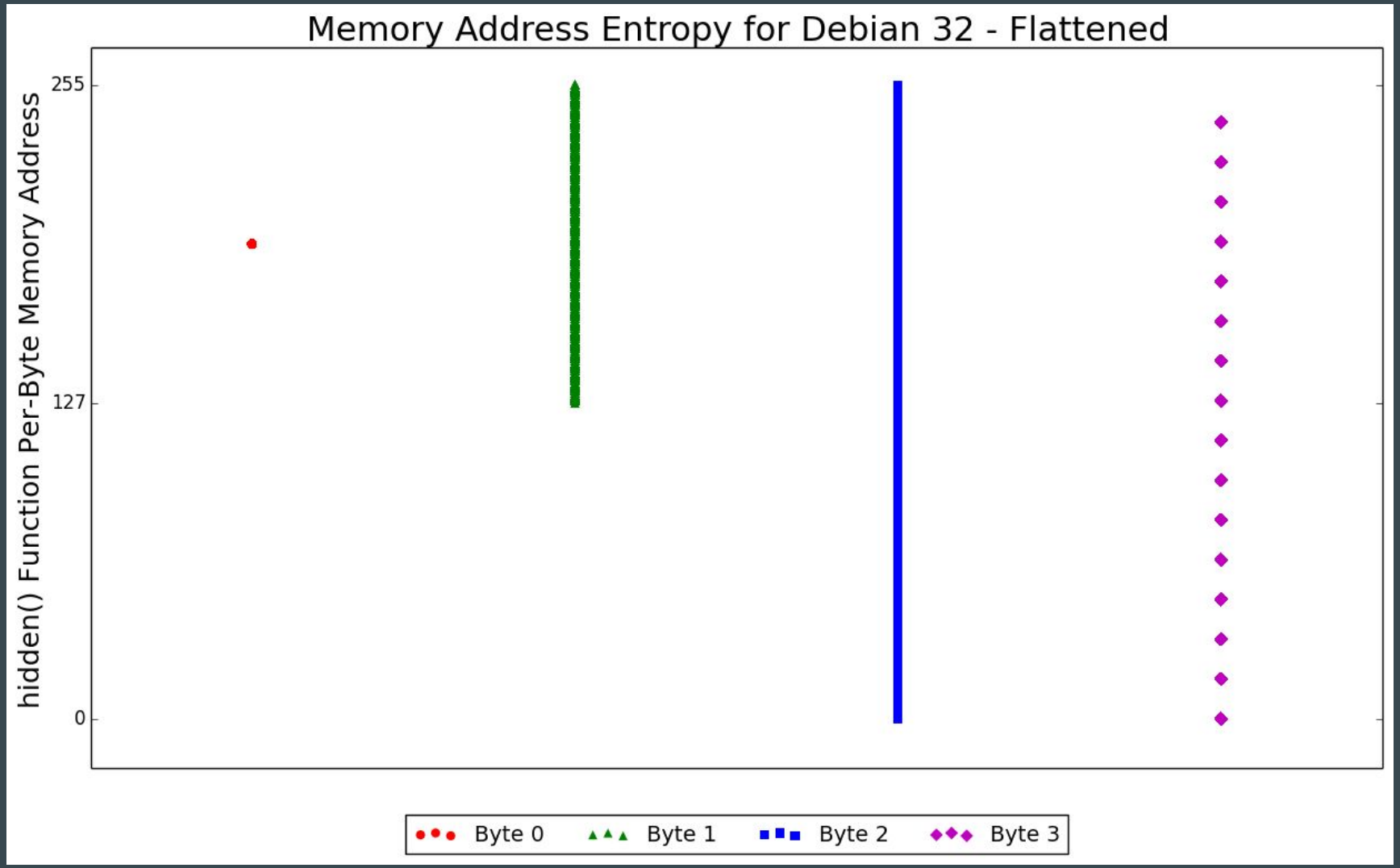
ASLR Results - 32-bit OpenBSD



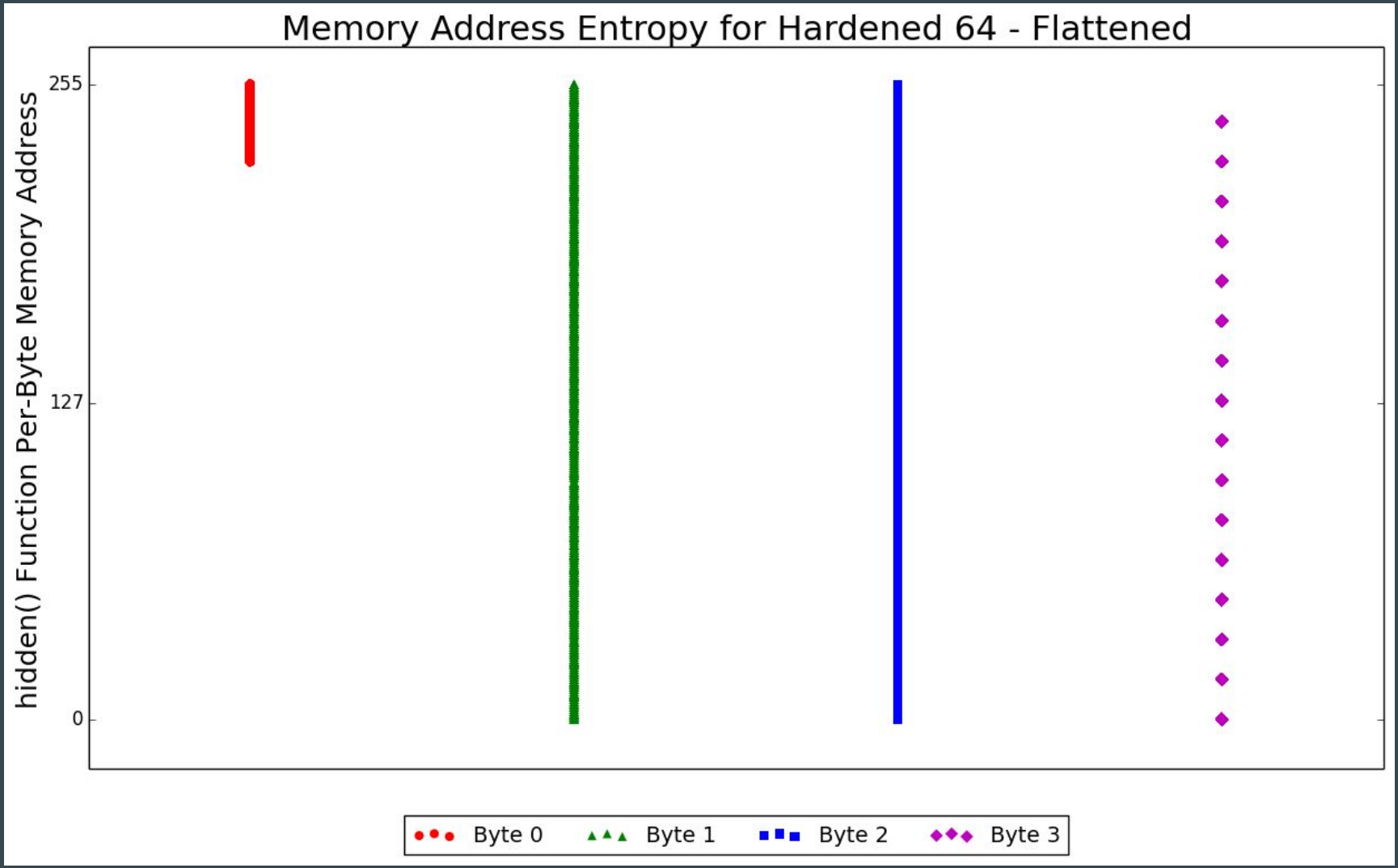
ASLR Results - 64-bit OpenBSD



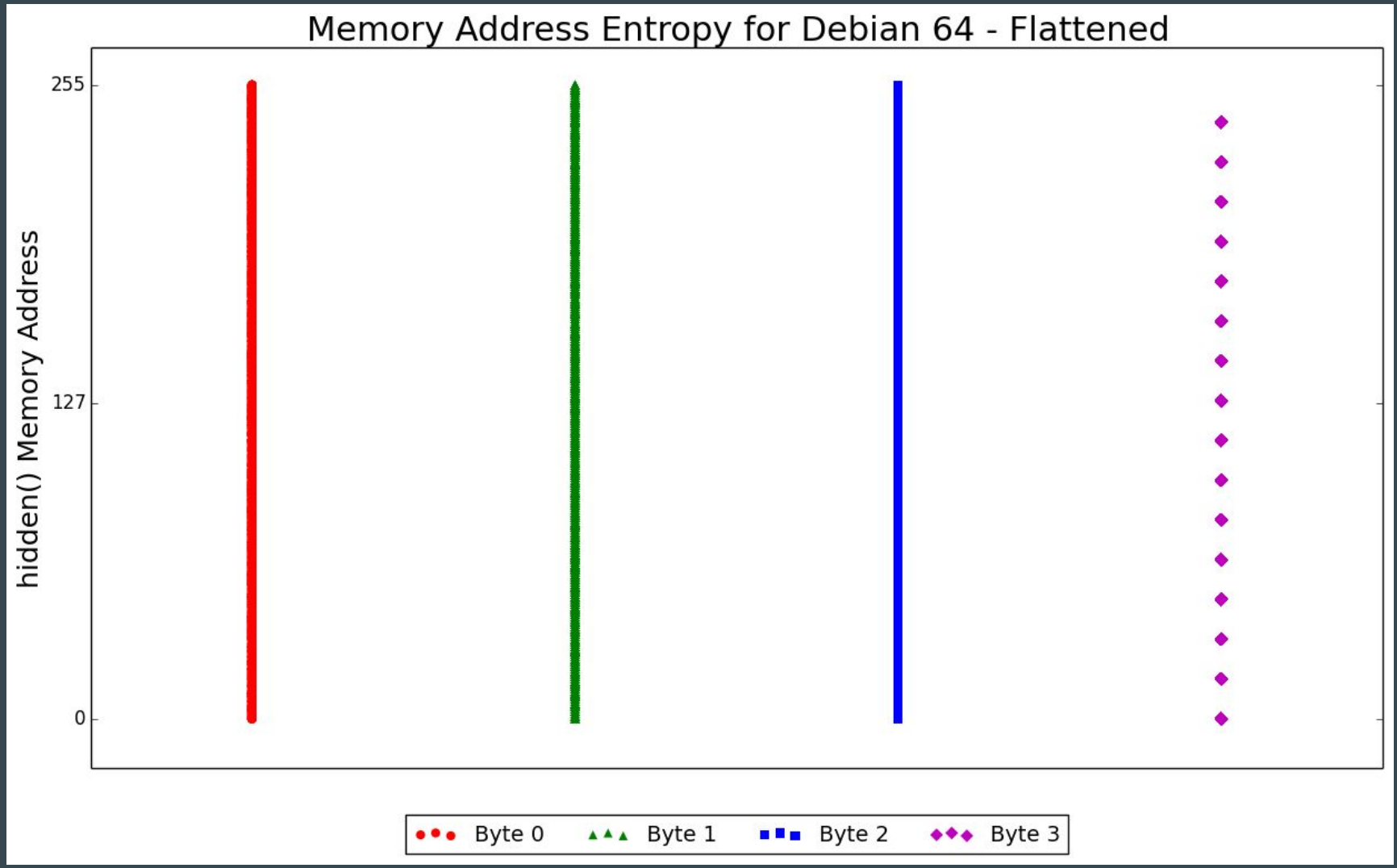
ASLR Results - 32-bit Debian Linux



ASLR Results - 64-bit HardenedBSD



ASLR Results - 64-bit Debian Linux



ASLR Results - Effective Entropy

	Claimed	Measured
64-bit Debian	28 bits	28 bits
64-bit HardenedBSD	30 bits	25 bits
32-bit Debian	24 bits	20 bits
64-bit OpenBSD	25 bits	15 bits
32-bit OpenBSD	16 bits	15 bits
32-bit HardenedBSD	14 bits	8 bits

Evaluation

- Debian (32-bit & 64-bit) ASLR Has Most Entropy
- 32-bit HardenedBSD ASLR Has Least Entropy
- *Operating Systems Often Provide Less Entropy than Claimed*
- We Must Perform Independent Tests of Security
- Evaluation Can Be Performed on More OSes

Limitations

- Small Set of Operating Systems Tested
  - Windows
  - macOS
  - Android
  - iOS
- Source Code Was Not Examined

Related Work

- “A Study of MAC Address Randomization in Mobile Devices and When it Fails” - Martin et al.
- “Techniques for the Dynamic Randomization of Network Attributes” - Chavez et al.

Conclusion

- Strength of Security Features Should Be Verified
- More Analysis Reveals Existing Limitations
- This Work Looks at Only One Defense Mechanism
- We Need More Quantitative Security Metrics

Questions?

www.jonganz.com

Security Research

- Malicious Media Sanitization
- Performance Analysis of Network Monitors
- Electronic Voting System Security Evaluation
- Multipath Routing Recovery Delay