Solving the Nixu Challenges 2019

Erik Sandberg
Patrick Richer St-Onge

The Challenges

- 19 challenges (for 2019)
- Main categories: forensics, reversing, web, network, crypto
- Motivation: fun, learning

Demo: Ports

Device Control Pawnage

- Insecure memory usage
- Part 1: Buffer overflow
- Part 2: Struct overflow

ACME Order DB

- Web
- 2 steps:
  - Bypass login screen
  - LDAP injection

Exfiltration

- pcap, analyzing web traffic
- File (PNG image) sent over network
- Sent in short snippets as part of DNS queries to a malicious server

Bad memories

Solved: 1, 3, 5 (out of 5)

- Forensics
- Memory dump of Windows 7 machine
- Recover text document, image, password, etc.

Ongoing challenges

- lisby (track of 3 challenges, reversing)
- AIMLES (pcap + pwn)
- fridge 2.0 (reversing + web)

Summary

- Currently solved 8/19 challenges, ranked #31 on the scoreboard
- The remaining challenges are harder, slower progress