AJPy: AJP python library
(or how to finally attack the port 8009 during pentests?)
Wait whaaaaat?

- Classic Java web application architecture

1. Send HTTP request
2. Translates HTTP request to AJP request and forward it

8009

Apache web server

Tomcat server
What is AJP?

- packet-oriented
- binary format (~ compressed HTTP)
- TCP connections reuse
- Current version: 1.3 (1998)
- About 42K open ports (tcp/8009) on the Internet (2012)
- Works with most of the Java application containers:
  - Apache Tomcat
  - JBoss/Wildfly
  - Jetty
  - Etc.
Security

- Many restrictions can be done on Apache web server
  - IP source filtering
  - Mutual SSL authentication
  - fail2ban
  - etc.

- Almost no restrictions on AJP Connectors
Hello, I speak AJP

Apache web server

1. Send HTTP request

2. Translates HTTP request to AJP request and forward it

Send AJP request

Tomcat server

8009

problem?
I don't really speak AJP

- AJPy is a small python library that can craft and serialize AJP packets
- Contains a tool for Tomcat
  - Get version (from error page)
  - Authentication bruteforce on admin panel
    BUT mitigated by LockOutRealm (>Tomcat 6)
  - WAR upload (almost) → webshell over AJP
Show time

IT'S TIME FOR YOUR
PURRFORMANCE REVIEW
Conclusion

- TODO
  - Fix the WAR deploy issue for Tomcat
  - Add JBoss/Wildfly support
  - Resource fuzzing
  - Improve and stabilize AJPy core library

- See you @BeeRump for more
  (CFP is still open, submit your papers @Baboon)