

# BAG-MuVAL 概要设计说明书

## BAG-MuVAL 概要设计说明书

项目整体结构

项目结构图

目标网络与OVAL扫描器模块

web 应用模块

MuVAL 模块

A2B 模块

用户交互

准备输入文件

访问 web 应用

输入内网信息文件

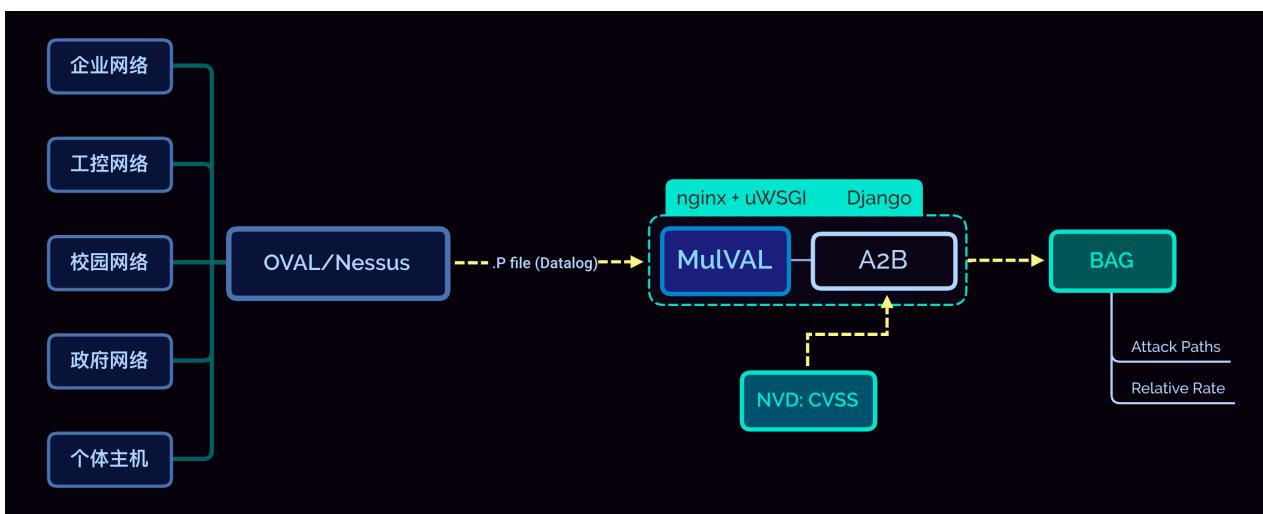
下载 MuVAL 生成的初始攻击图

选择一个攻击目标生成贝叶斯攻击图

输出解读

## 项目整体结构

## 项目结构图



## 目标网络与OVAL扫描器模块

本模块不属于本项目 *web* 应用 *BAG-MuVAL*，但是是 *BAG-MuVAL* 的输入来源。首先使用 *Nessus* 等 OVAL（开放式漏洞评估语言）扫描器对要分析的各种网络进行扫描。扫描得到的信息越多，最后的分析越充分完整。将扫描得到的网络配置信息、漏洞信息、主机互连信息写成 *Datalog* 的事实和结果语句<sup>1</sup>，即 *.P* 文件，通过网络传输到 *BAG-MuVAL* *web* 应用上进行分析。

## web 应用模块

*web* 应用包含两个模块，即 **MulVAL** 和 **A2B**。

## MulVAL 模块

接收到 *.P* 文件后，先调用 **MuVAL** 生成初始的属性攻击图与其 *XML* 文件。

A2B 模块

调用 **A2B** 模块解析攻击图的 *XML* 文件，分析并处理攻击图；同时通过爬虫爬取到的 *NVD CVSS* 信息查询攻击图中所有漏洞的各项 *CVSS* 评分，用于计算各攻击路径的贝叶斯概率。

最后调用 *Python* 库 *Graphviz* 生成可视化贝叶斯攻击图，包含可能的攻击路径及路径对应的相对攻击成功概率。

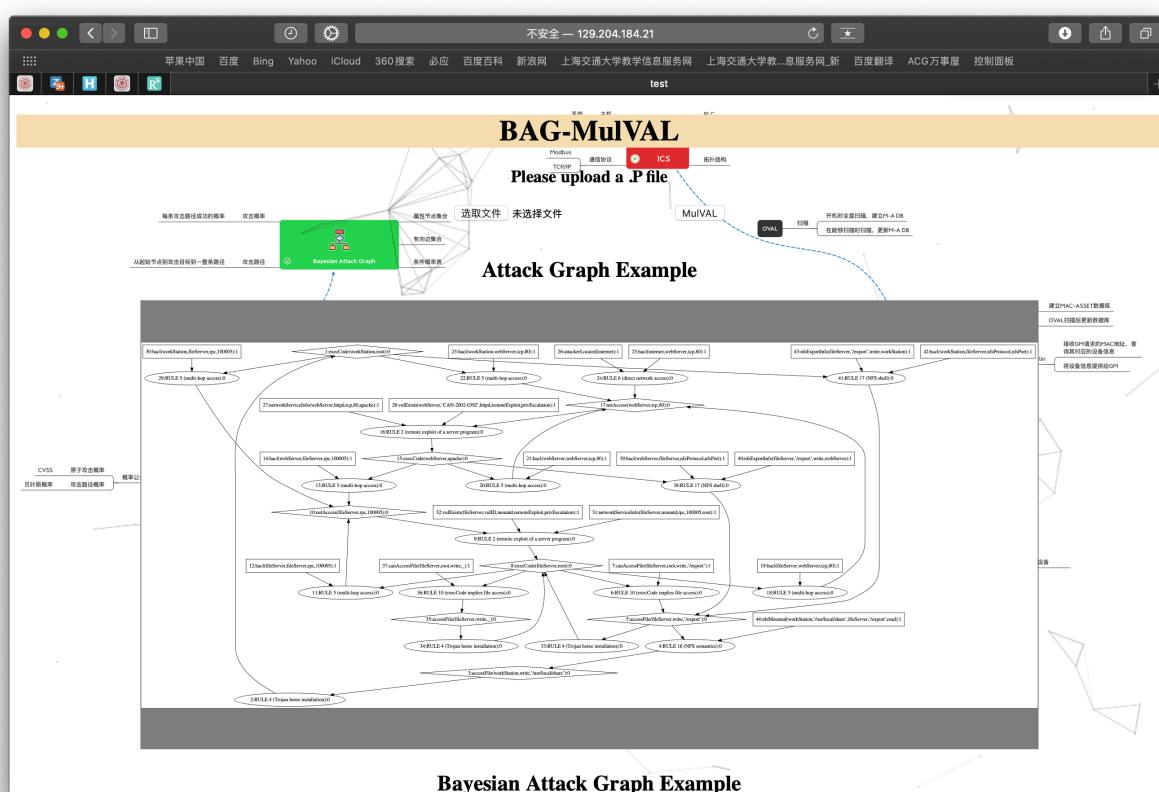
## 用户交互

## 准备输入文件

用户通过 *Nessus* 等扫描器得到待分析网络的漏洞信息、主机互连信息、配置信息，生成输入文件。

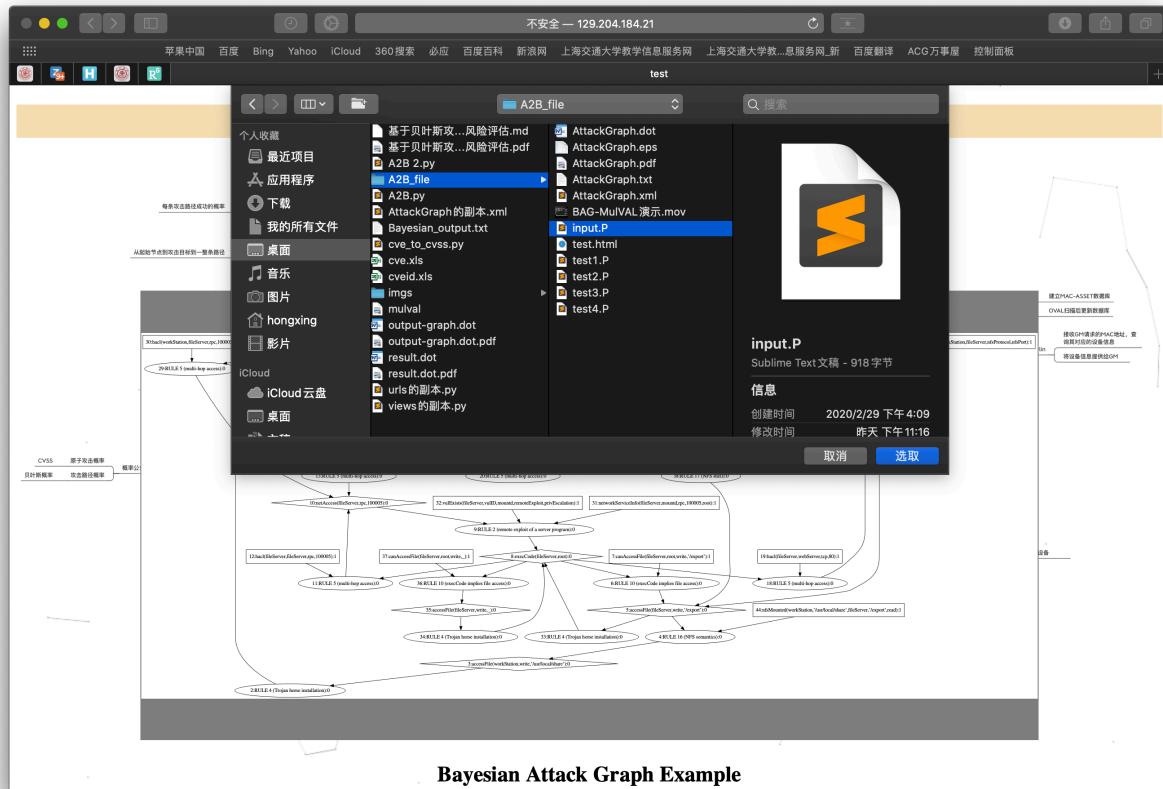
## 访问 web 应用

打开浏览器，访问公网地址：<http://mekakuactor.cn/mulval/window/>

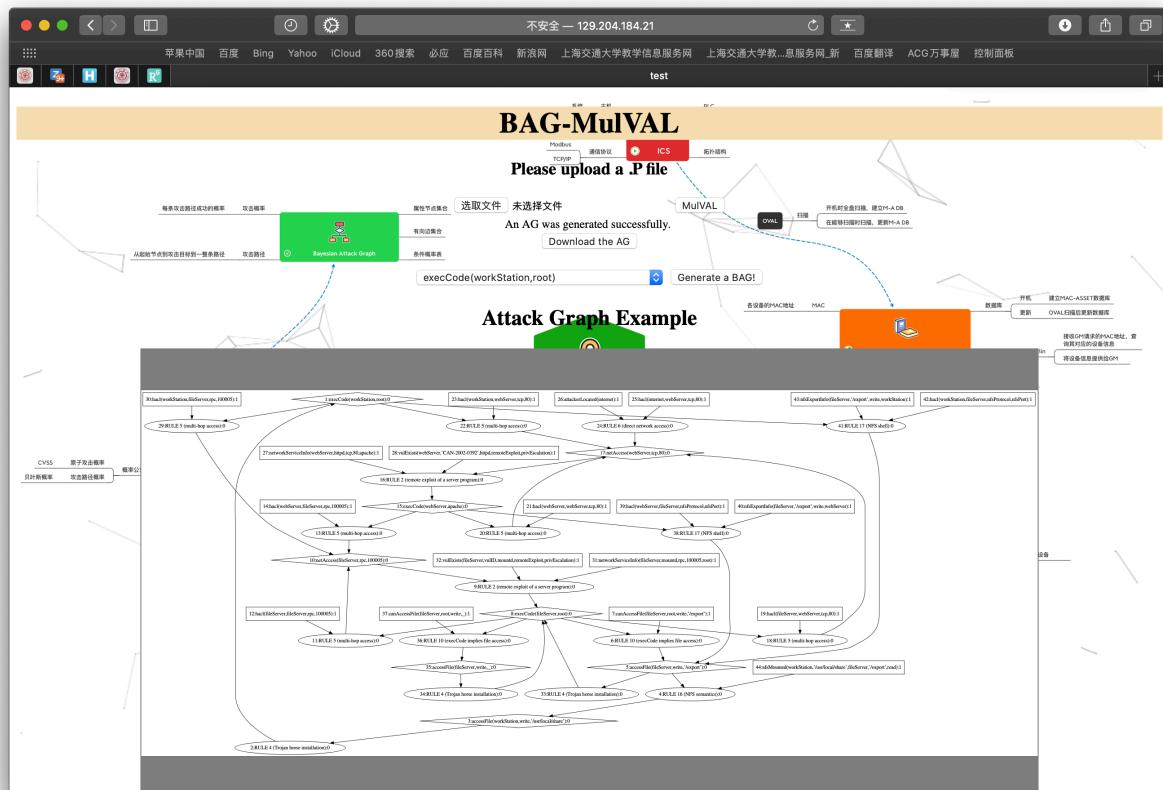


## 输入内网信息文件

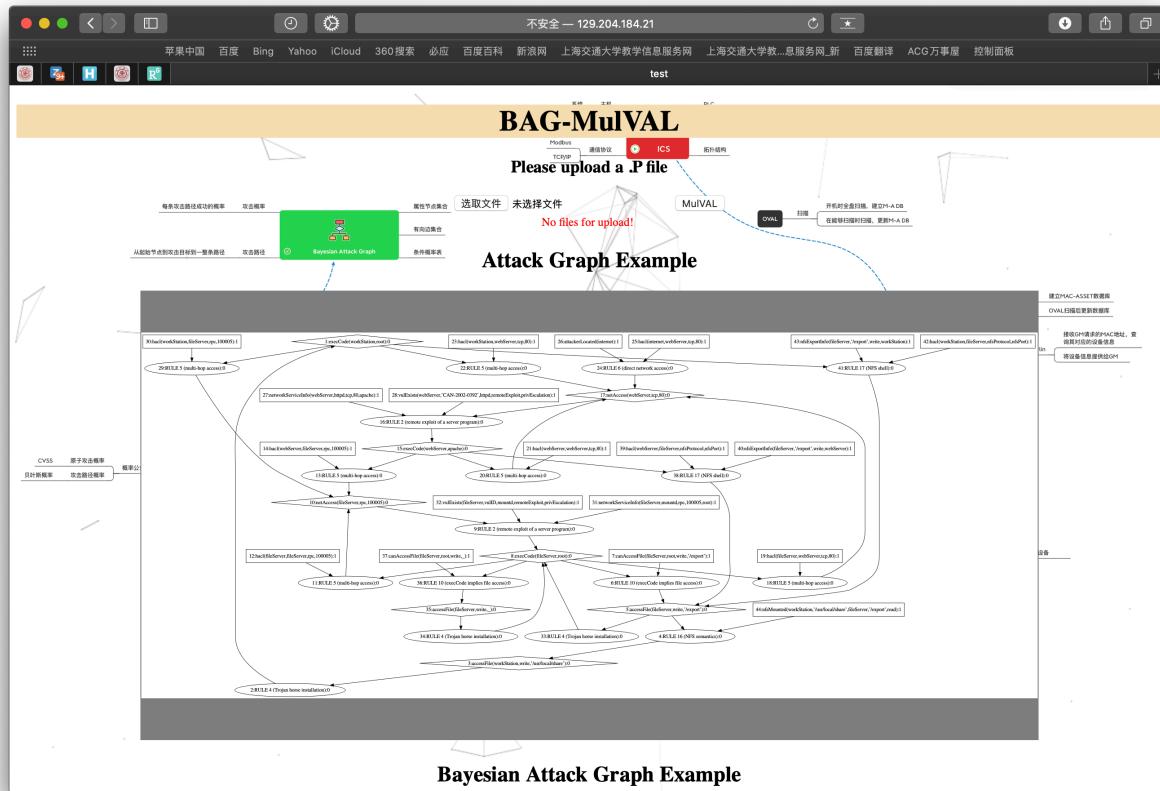
点击“选择文件”，选择上传之前准备好的文件。点击 “MulVAL”，生成初始攻击图，出现 “An AG was generated successfully.” 的提示信息，并出现多个新按钮。



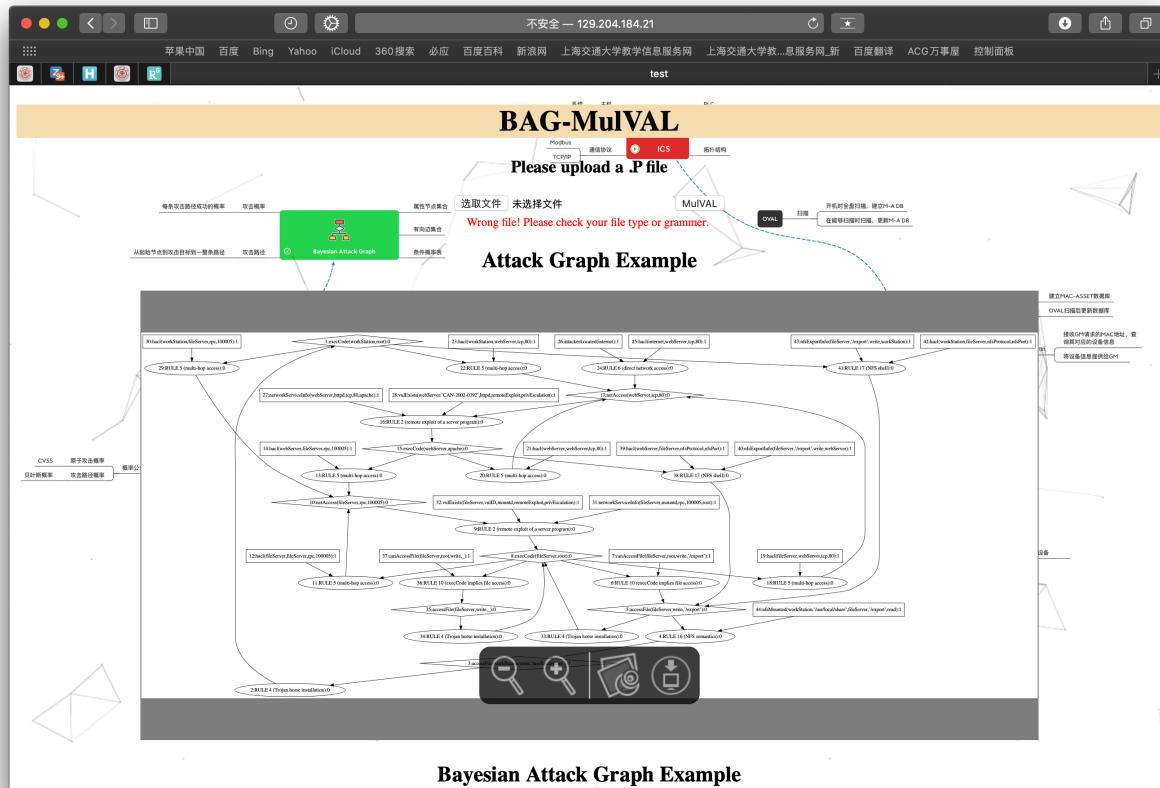
Bayesian Attack Graph Example



如果上传空文件，会出现 “No files for upload!” 的提示错误信息。



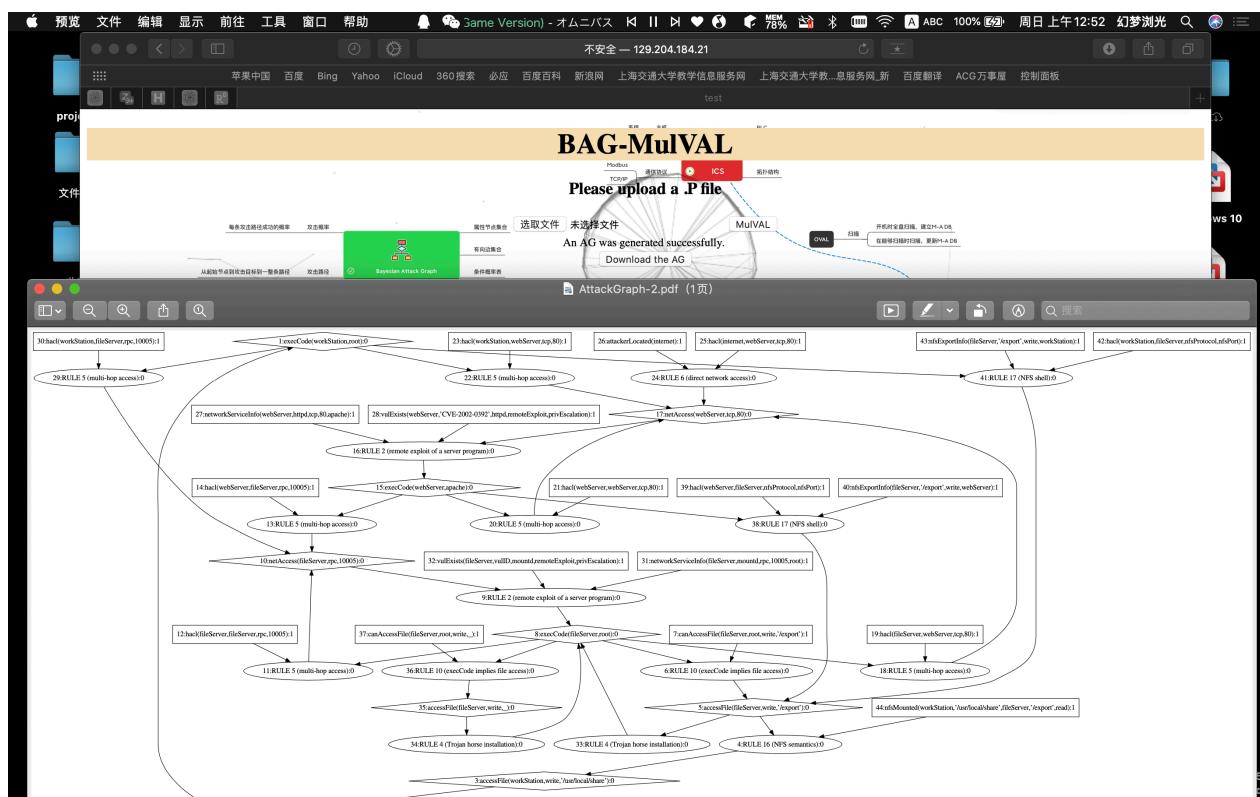
如果上传文件类型错误或不符合语法，会提示 “*Wrong file! Please check your file type or grammer.*” 错误信息。



如果 **MulVAL** 找不到攻击路径，说明该网络安全性良好，会提示 “*No attack path found.*” 信息。

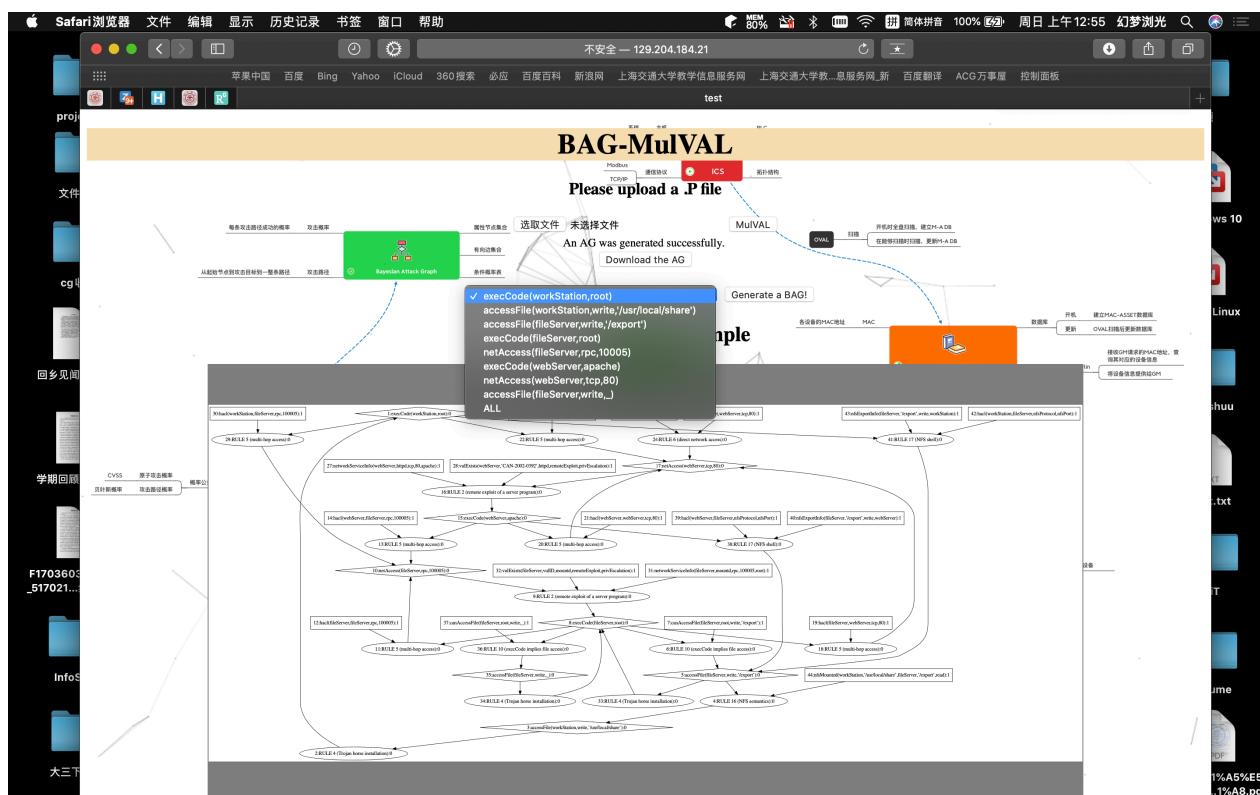
# 下载 MulVAL 生成的初始攻击图

点击新出现的 “Download the AG” 按钮，下载刚刚成功生成的攻击图。

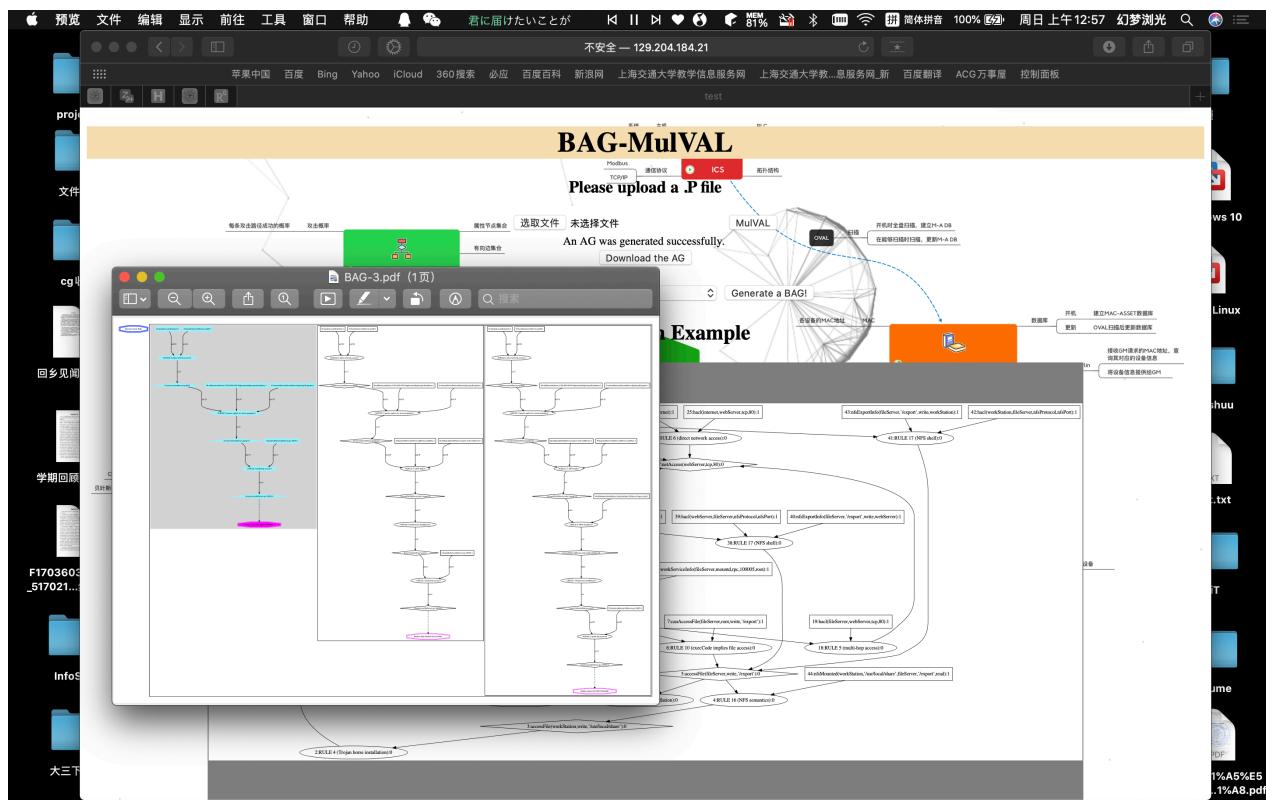


## 选择一个攻击目标生成贝叶斯攻击图

在选择栏里选择一个攻击目标，攻击目标指在内网中获得一种权限或能力。



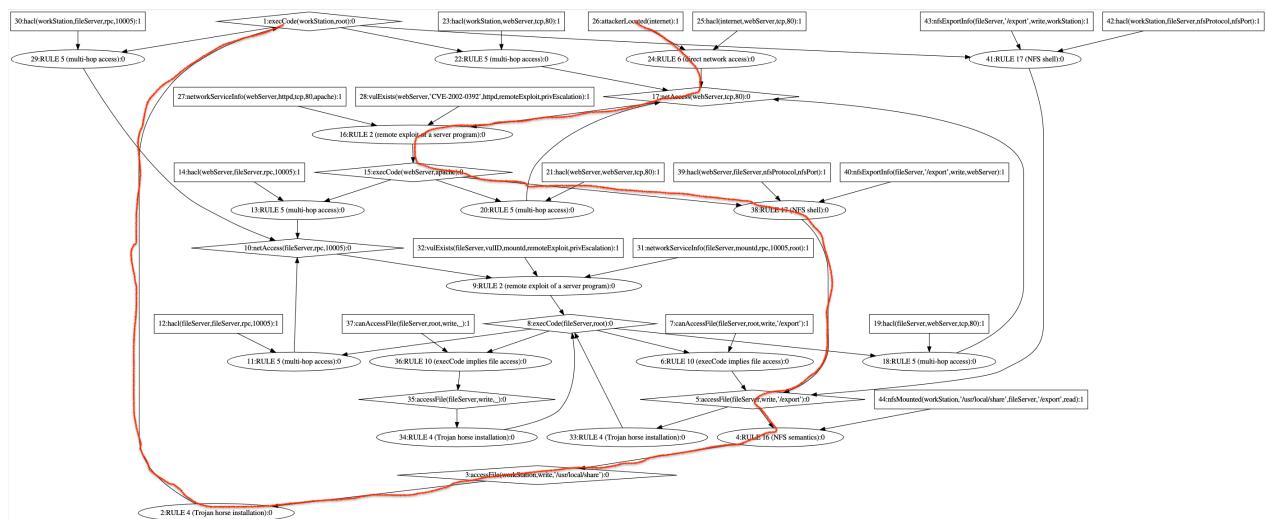
点击 “Generate a BAG”，生成并下载贝叶斯攻击图。

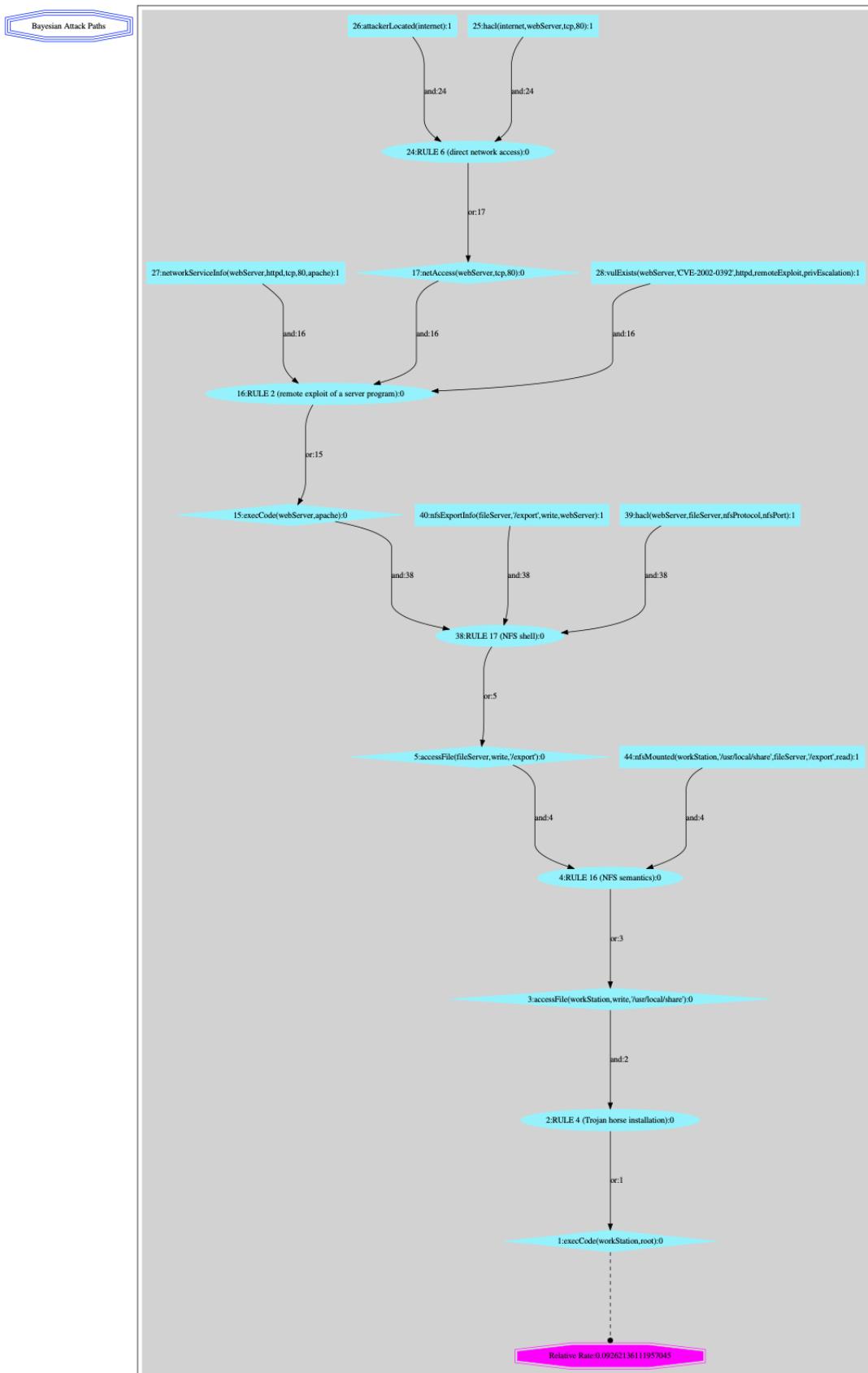


该贝叶斯攻击图包含从攻击者到攻击目标的所有独立的攻击路径，及各攻击路径的相对攻击成功概率。相对攻击成功概率最高的路径以颜色标示。攻击路径与攻击概率将辅助网络管理员对网络安全态势进行判断，并帮助网络管理员对如何提升网络安全性进行决策。

## 输出解读

为了帮助读者更好地理解 **A2B** 模块的作用，下面展出了两张图，前者是 **MulVAL** 模块生成的初始攻击图，后者是再经过 **A2B** 模块处理后生成的贝叶斯攻击路径，其在前一张图中以红线标出。可见本项目能正确地生成内网的攻击图，并分析处理该攻击图，生成贝叶斯攻击图，包含清晰的攻击路径以及该路径的相对攻击成功概率。攻击路径与攻击概率将辅助网络管理员对网络安全态势进行判断，并帮助网络管理员对如何提升网络安全性进行决策。





1. 基于 Datalog 的知识推理. <https://blog.csdn.net/oangoaog/article/details/78932517> ↵