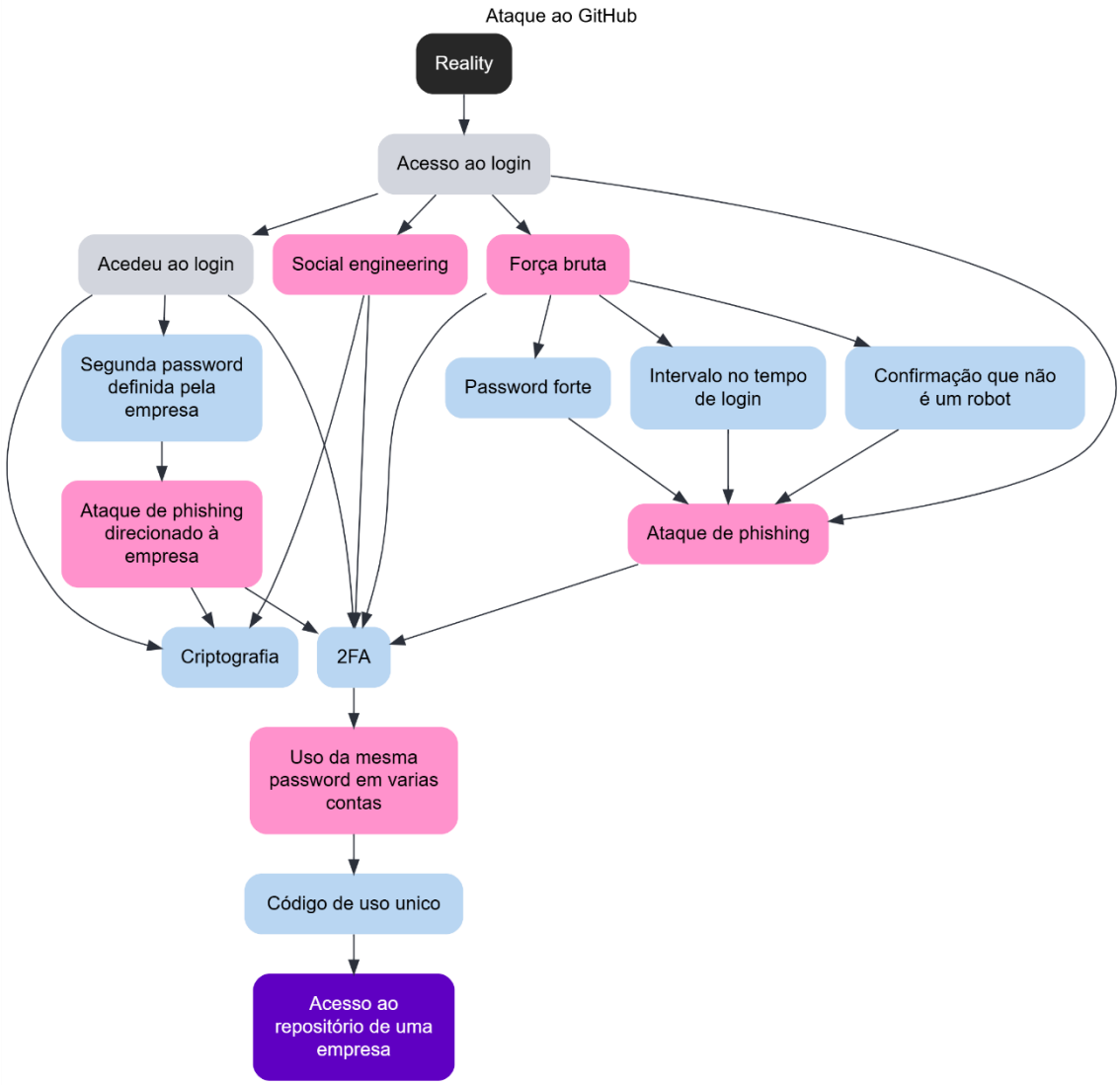
RSI – Redes e Segurança Informática

Paulo Carvalho – nº 85569

Parte I

Ataque ao GitHub

A minha Árvore de Ataque dedica-se às possíveis rotas para entrar no repositório de uma empresa e aceder a informações privadas sobre o código da mesma.



Podemos deduzir pelo gráfico acima que ataques de *phishing* acabam por ser as melhores ferramentas para ultrapassar as várias mitigações possíveis. Do outro lado, podemos conferir que autenticação de 2 fatores acaba por ser o fim de vários ataques (incluindo o *phishing*).

É preciso também indicar que, a partir do momento em que o atacante ultrapassa a primeira barreira (login de um colaborador), a melhor estratégia seria criptografia com uma chave escondida na empresa que só o colaborador conhecesse - algo que também poderia ser atacado com *phishing* especializado para os emails de empresa, voltando de novo a talvez mais uma autenticação de 2 fatores (dependendo da importância do conteúdo).

Parte II

CSIRT – Banco de Portugal

O CSIRT-BDP (Computer Security Incident Response Team do Banco de Portugal) é a unidade responsável pela prevenção, deteção e resposta a incidentes de cibersegurança no Banco de Portugal. A sua missão é proteger os interesses, o negócio e a reputação da instituição contra ameaças digitais, assegurando a confidencialidade, integridade e disponibilidade da informação.

A atuação do CSIRT-BDP abrange todos os componentes do ecossistema tecnológico do Banco, incluindo utilizadores, sistemas, aplicações, infraestruturas e funções de negócio suportadas por tecnologia. A equipa desenvolve atividades de monitorização contínua, análise de eventos de segurança e resposta coordenada a incidentes, procurando minimizar impactos e restaurar rapidamente a normalidade operacional.

Entre os principais serviços prestados destacam-se a resposta a incidentes, a análise forense digital e a identificação e comunicação de vulnerabilidades. Para além da vertente reativa, o CSIRT-BDP assume também um papel preventivo, promovendo boas práticas de segurança e contribuindo para o reforço da cultura de cibersegurança dentro da organização. Localizado em Lisboa, privilegia o contacto por email para reporte de incidentes e coordenação de respostas.