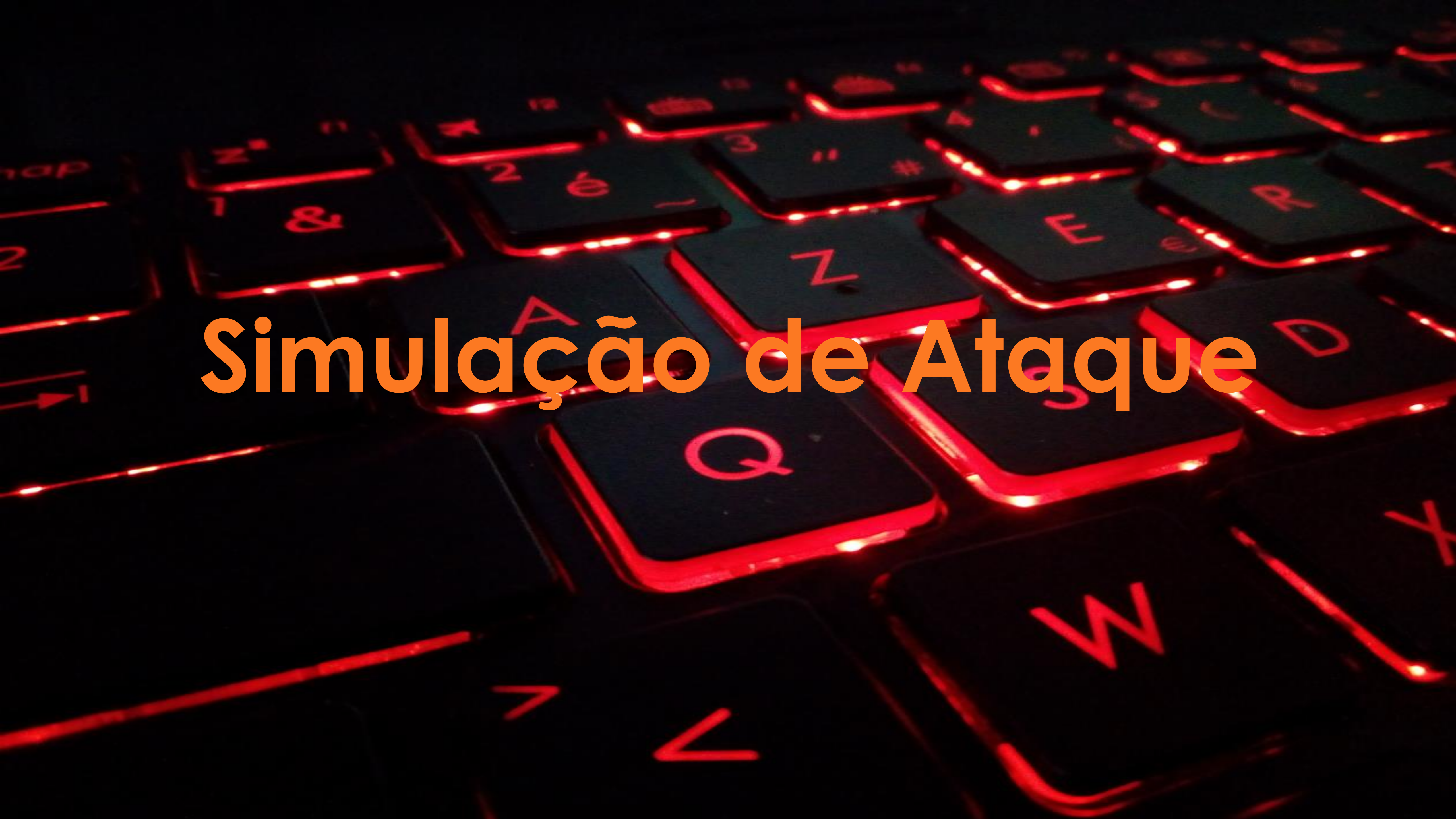
Simulação de Ataque



Integrantes

- Washington W.
- Luiz H.
- Lucas H. Ignácio

Simulação de Ataque a sites e outras redes

- Procura identificar ameaças e vulnerabilidades e brechas que possam ser exploradas por usuários maliciosos, através da realização de simulações de ataque;
- Os testes podem ser originados interna ou externamente;
- Os auditores podem ou não ter acesso a informações sobre a estrutura (definição se o teste será do tipo "caixa preta" ou "caixa branca");
- Auditores são pessoas que trabalham na Auditoria de Teste Invasão.

Técnicas que geralmente são utilizadas

- **Sondagem e Mapeamento**
  Consiste na varredura por hosts ativos, mapeamento de topologia e regras de firewall e detecção de serviços em execução.
- **Força Bruta**
  Visa detectar serviços de autenticação ou controle de acesso vulneráveis a ataques de tentativa e erro de senhas. Analisa a qualidade da política de senha e de sua implementação.
- **Análise de Tráfego de rede**
  Verifica se é possível identificar e obter informações sensíveis através da manipulação de tráfego de rede.
- **Avaliação de Servidores Web**
  Busca as principais vulnerabilidades em serviços deste tipo. Manipula requisições de modo a tentar comprometer a segurança de serviços web.
- **Identificação e Exploração de Vulnerabilidades**
  Lança códigos maliciosos visando explorar as vulnerabilidades identificadas.

8° Ferramentas de Simulação de Ataque

- **Metasploit**
- **Nessus Vulnerability Scanner**
- **Nmap**
- **Burp Suite**
- **OWASP ZAP**
- **SQLmap**
- **Kali Linux**
- **Jawfish**

A ferramenta mais utilizada entre elas é o

KALI LINUX

O Kali Linux

- O Kali Linux é um sistema operacional Linux baseado no Debian, que é desenvolvido pela pequena e consagrada equipe da Offensive Security;
- É gratuito e sempre será;
- Ele contem mais de 300 ferramentas nativas para testes de invasão, penetração, força bruta, forense entre outras;
- Atualmente é um dos sistemas mais famosos no mundo na área de segurança da informação;
- Ele é muito utilizado por hackers, pentesters, analistas e auditores de segurança da informação.

Simulação de ataque ajuda ou atrapalha

- OS programadores do Comando de Defesa Aeroespacial da América do Norte (NORAD) quase iniciaram a Terceira Guerra Mundial, quando eles acidentalmente rodaram um programa que simulava um ataque soviético. De acordo com o NORAD, a União Soviética havia acabado de lançar 250 mísseis cujo destino final seria o solo americano. Brzezinski recebeu outra ligação pouco tempo depois da primeira, e nela o NORAD reportava que não eram 250 mísseis, mas 2.200. Este foi o momento que todo americano que viveu durante a Guerra Fria temia. E os oficiais não planejavam avisar o público.

Conclusão

- Concluímos que a simulação de ataque ela não só ajuda, mas também pode atrapalhar por conta de seus próprios equipamentos que são utilizados para testar a segurança, serve para hackers que utilizam para hackearem.