

Conclusão da aula

Transcrição

Nós conseguimos realizar os ataques dos hubs com o WireShark, conseguindo visualizar não apenas os sites que o João estava acessando, mas também seu usuário e senha. Depois, fizemos os ataques de switch, com o `mac overflow` e o `GNS3`.

A seguir, passamos para o ataque *Man in the Middle*, ficando no meio da comunicação entre dois dispositivos. Também fomos capazes de alterar o redirecionamento DNS com o DNS Spoofing.

Fizemos ataques do lado do servidor, como o *Denial of Service* e o `slowloris`, abrindo uma série de conexões com o servidor. Conseguimos também ver suas vulnerabilidades com o Nessus, e rodamos um exploit para verificar a questão do `open SSH`, indicada por ele.

Além disso, fizemos um ataque do lado do cliente, no qual criamos um vírus, para ilustrar o que pode acontecer.

Espero que com isso eu tenha conseguido ajudá-lo a entender o que pode vir a comprometer uma rede, quais são os tipos de ataque possíveis. Agradeço por ter chegado ao fim do curso e espero vê-lo em uma próxima oportunidade. Até lá!