

03

## Mão à obra: Explorando vulnerabilidades

Descobrimos com o Nmap os serviços que estão rodando em nosso servidor, na análise, descobrimos que o servidor possui a porta 21 aberta e que a versão referente a esse serviço seria **vsftpd 2.3.4**.

Vimos no vídeo que essa versão apresenta uma vulnerabilidade, vamos explorá-la com um framework que possui vários códigos com o intuito de explorar vulnerabilidades, os exploits. Temos no Kali Linux o Metasploit, que possui já pré instalado uma série de exploits. Vamos explorar a vulnerabilidade dessa versão com o objetivo de ganhar acesso do servidor.

- No Kali Linux, abra o Metasploit



- Selecione o exploit que iremos usar para explorar essa vulnerabilidade, digitando: **use exploit/unix/ftp/vsftpd\_234\_backdoor**
- Configure o alvo do teste: **set RHOST [IP do servidor]**
- Rode o código digitando: **exploit**

Qual foi o resultado?