Essa atividade não está no quadro da sprint. Representa

o ataque à porta RPC descoberta na análise de servidor - nmap.

**Data**: 10-04-16.

**Tempo usado no teste**:1h

**Tempo total**: 1h

**Objetivo**: Tentar se conectar à porta 135 usando o framework metasploit para tentar conseguir privilégios dentro do windows.

**Ferramenta:** Metasploit é um framework de intrusão que é carregado com muitos payloads e exploits automatizados que facilitam alguns testes.

**Resultados**

**Tentativa 1:**

**Resultado:**

A ferramenta é de dificil configuração e possui documentação muito ruim. Não consegui grandes resultados.

**Tentativa 2:**

**Resultado**: consegui mandar um exploit mas não trouxe resultado.

fui verificar e o exploit é pra windows NT.

O exploit escolhido foi o *auxiliary/scanner/msf/msf\_rpc\_login* para

testar o caso específico da porta RPC escolhida. O payload a ser executado

é o *windows/meterpreter/reverse\_tcp.* Esse payload força a máquina atacada a abrir uma conexão com a máquina atacante via TCP.

**Tentativa 3:**

Tentar atacar a porta 445 usando exploits automatizados.

Para esse caso o exploit escolhido foi o MS08-67 disponivel no caminho */windows/smb/ms08\_067\_netapi.* Ele serve especificamente para explorar uma vulnerabilidade do microsoft ds. O payload é o mesmo do teste passado: *windows/meterpreter/reverse\_tcp.* Esse payload força a máquina atacada a abrir uma conexão com a máquina atacante via TCP.

**Resultado**: Passou no teste

**Tentativa 4:**

tentar atacar a porta 135

O exploit escolhido foi o *auxiliary/scanner/msf/msf\_rpc\_login* para

testar o caso específico da porta RPC escolhida. O payload a ser executado

é o *windows/meterpreter/reverse\_tcp.* Esse payload força a máquina atacada a abrir uma conexão com a máquina atacante via TCP.

**Resultado**: Passou no teste