08

Mãos à obra: Testando vulnerabilidade OpenSSH

Pela varredura que o Nessus realizou, descobrimos que a versão do OpenSSH apresenta uma vulnerabilidade na geração das chaves, documentada na Common Vulnerabilities and Exposure (CVE) com a referência 2008-0166.

Ao procurar por essa referência descobrimos que existem códigos exploits para essa vulnerabilidade. Vamos explorar essa vulnerabilidade que foi descoberta pelo Nessus:

- No Kali Linux, vá ao browser e acesse este link (https://www.exploit-db.com/exploits/5720/).
- Na aba exploit, clique em **Download**
- Ao ler a documentação do autor do código temos os passos a serem executados para realizarmos o ataque:
  - Abra uma outra aba no browser e realize o download das chaves neste link (https://drive.google.com/open?id=0BzmYQVmw4W7nOElJaFFWdm1DODg). (Obs: cuidado ao realizar download de exploits na internet).
  - No terminal do Kali Linux, altere para o diretório onde os arquivos foram salvos, por exemplo **cd Downloads/**
  - Faça a extração do arquivo, digitando: **bunzip2 5622.tar.bz2** e posteriormente digite: **tar xvf 5622.tar**
  - Execute o ataque digitando no terminal: **python 5720.py [*caminho completo onde o diretório com as chaves foram salvos] [IP do servidor] root 22**
  - O processo poderá demorar. A chave foi encontrada? Tente rodar o comando e ver se o acesso ao servidor é obtido.

*Exemplo de caminho completo das chaves: `/root/Downloads/rsa/2048/ .`