

Atividade 01 – PenTeste

Individual

Realizar um PenTeste na VM (**vitima2023.ova**) disponível no link:

- https://drive.google.com/file/d/1b2iDvSR8AipW2rTOEu32wRiDobqJUZqN/view?usp=share_link

Neste PenTeste, você deve realizar no mínimo os passos que fizemos em sala de aula (Escaneamento e Ganhando Acesso), principalmente utilizando as ferramentas Nmap, Metasploit, SQLmap e Hydra/John the Ripper. Todavia, você não deve ficar restrito à essas ferramentas ou passos. Ou seja, tente descobrir o maior número possível de vulnerabilidades nesta VM. Atenção, você só deve realizar o PenTeste via rede, não deve utilizar técnicas offline, como dar “boot” com outro Linux/SO.

Ao final você deve entregar no Moodle da disciplina um texto com:

1. Introdução a respeito de PenTeste (passos, principais ferramentas);
2. Descrição a respeito do PenTeste que você realizou (todos os passos, comandos e resultados obtidos – utilize *screenshots*, mas sempre disserte a respeito do que você fez);
3. Relatório detalhando tudo o que foi descoberto no PenTeste (imagine que seja o relatório para um cliente real).
4. Conclusão a respeito das aulas a respeito de PenTeste, do PenTeste realizado por você, das facilidades e dificuldades durante o PenTeste.

Atenção, tente fazer o PenTeste por você mesmo (não copie). Nesta atividade o professor não vai dar mais nota ou menos nota, pela quantidade de vulnerabilidades que você descobriu no PenTeste. A nota estará relacionada aos procedimentos e passos que você realizou (não o resultado) e principalmente a nota está diretamente relacionada com o relatório de PenTeste que você produziu (qualidade do texto, imagens, explicações, etc).