



PROFESSOR: Daniel Caetano
DISCIPLINA: ARA0076 – Segurança Cibernética

INSTRUÇÕES

- a) A atividade é em **grupo!** Apenas um dos alunos do grupo precisa entregar!
- b) Inclua os nomes e RAs de todos os membros do grupo na primeira página do relatório!
- e) Grave o relatório no formato **PDF** e entregue-o pelo **TEAMS** (menu “Trabalhos”) até **29/05/2022**.
- f) O trabalho, entregue até a data, vale 2,5 na AV2. Cada dia de atraso ocasionará um desconto de 0,5 nessa nota.

ATIVIDADE AVALIATIVA C – AULA 10 (2,5 NA AV2)

- 1) Pesquisa por 3 CVEs em https://cve.mitre.org/cve/search_cve_list.html

Sugestão: CVE-2002-0283, CVE-2010-0816, CVE-2020-15708

- 2) Pesquise também aqui: <https://www.cvedetails.com/>

- 3) Baixe e instale o Packet Tracer em seu computador. É necessário login com a conta do Cisco Network Academy

- 4) Verifique se encontra a solução publicada pelo fornecedor. Por exemplo, nos sites:

Windows: <https://msrc.microsoft.com/update-guide>

Ubuntu: <https://ubuntu.com/security/cve>

Debian: <https://security-tracker.debian.org/tracker/>

RedHat: <https://access.redhat.com/security/security-updates?cwe=476#/cve>

- 5) Analise e compreenda a falha e as correções divulgadas.

- 6) Elabore um texto técnico explicando de forma clara a vulnerabilidade e como as correções ocorreram.

DICA: Os sites indicados estarão todos em inglês. Sugestão: entre em <https://translate.google.com/> e copie o endereço da página em inglês na caixinha da esquerda; selecione a língua “Português” sobre a caixinha da direita. O link aparecerá na caixinha da direita. Clique no link da caixinha da direita. A página abrirá traduzida.