



**PROFESSOR:** Daniel Caetano  
**DISCIPLINA:** ARA0076 – Segurança Cibernética

#### **INSTRUÇÕES**

- a) A atividade é **individual!**
- b) A entrega é apenas do relatório final!
- c) Inclua seu nome e seu RA na primeira página do relatório!
- e) Grave o relatório no formato **PDF** e entregue-o pelo **TEAMS** (menu “Trabalhos”) até **01/11/2021**.
- f) O trabalho, entregue até a data, vale 2,5 na AV2. Cada dia de atraso ocasionará um desconto de 0,25 nessa nota.

### **ATIVIDADE AVALIATIVA B – AULA 09 (2,5 NA AV2)**

- 1) Baixe o WireShark ( <https://www.wireshark.org/> ) e instale-o em seu computador.
- 2) Usando técnicas de Google Hacking, encontre algum site que não faça uso de criptografia (ou seja, que use protocolo HTTP).
- 3) Acesse o site e capture os pacotes desse site pelo WireShark (se necessário, relembre o uso do WireShark vendo o vídeo da Aula 04).
- 4) Analise os pacotes e veja se consegue identificar o texto da página nos pacotes; tente encontrar alguma informação interessante (dados de login, senha, informações sobre sessão, cookies...)
- 5) Procure agora um site que use criptografia (HTTPS – a maioria dos sites atuais usa).
- 6) Acesse o site e capture os pacotes desse site pelo WireShark.
- 7) Analise os pacotes e veja se consegue identificar o texto da página nos pacotes; tente encontrar alguma informação interessante (dados de login, senha, informações sobre sessão, cookies...)
- 8) Na forma de um relatório, documente o procedimento realizado e os resultados obtidos, bem como suas conclusões sobre a proteção que o protocolo HTTPS traz para a comunicação entre o navegador e o servidor web. Use imagens do navegador e do wireshark para enriquecer o seu relatório. Esse relatório será a entrega do trabalho.