ETSC - Emulador para Treinamento em Segurança Cibernética

Universidade Federal de Campina Grande – UFCG

Demo Day

Novembro de 2024

Equipe

Edmar C. Gurjão

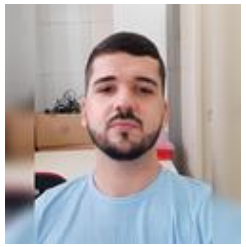
Leocarlos B. S. Lima

Matheus Vilarim

Bárbara Barbosa

Ana Júlia

Fernando Barros



João Paulo

Lucas R. Albino

Laura Delai

Motivação

Necessidade

- Treinamento *hands on*: **custo alto;**
- Simulação: **virtualização;**
- Necessidades:
  - Baixo custo;
  - Ambiente Controlado;
  - Ajustável ao público;
  - Escalável.

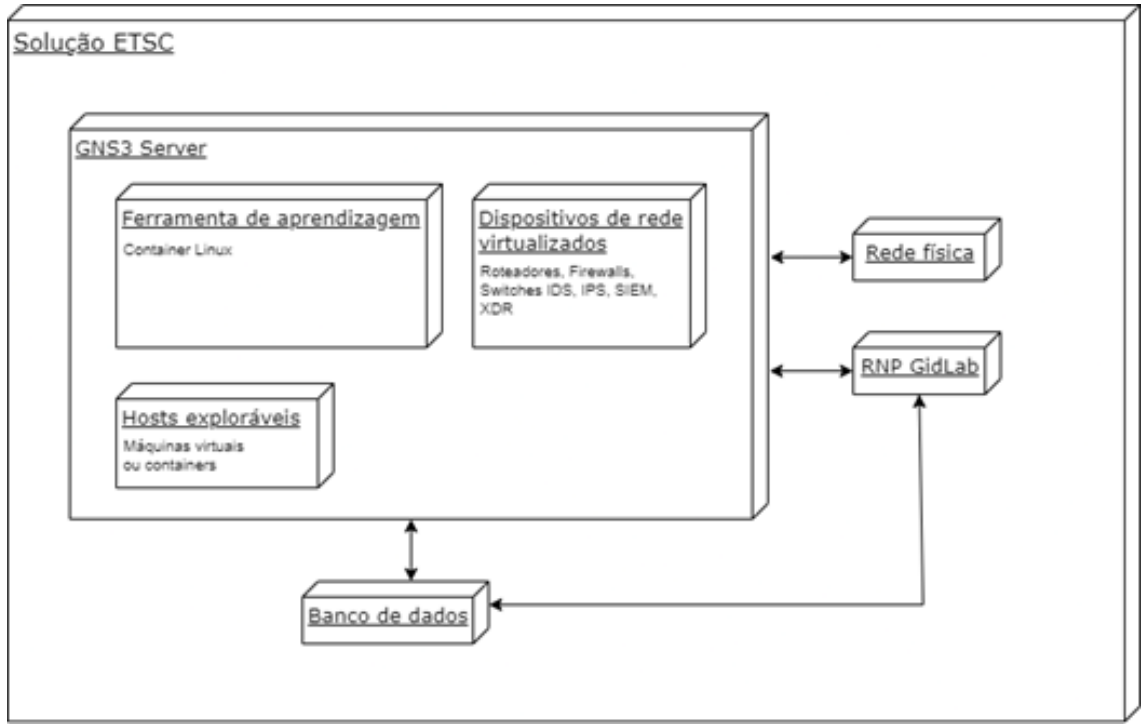
Projeto

Desenvolvimento e a implementação de um emulador de cenários de segurança cibernética.

Solução

Plataforma de cursos, com módulos configuráveis para treinamentos em segurança cibernética de forma segura e escalável.

Introdução e Contextualização do Projeto



Arquitetura da topologia proposta

i. **Simulador GNS3:** gratuito e possibilidade de uso de contêineres;

ii. **Ferramenta de aprendizagem:** cenários distintos (disponibilizados de forma aleatória) em execuções distintas;

iii. **Banco de Dados:** repositório com cenários;

iv. **Acesso à rede física:** integração com rede local ou dispositivo físico;

v. **Integração com o GidLab.**

Definições

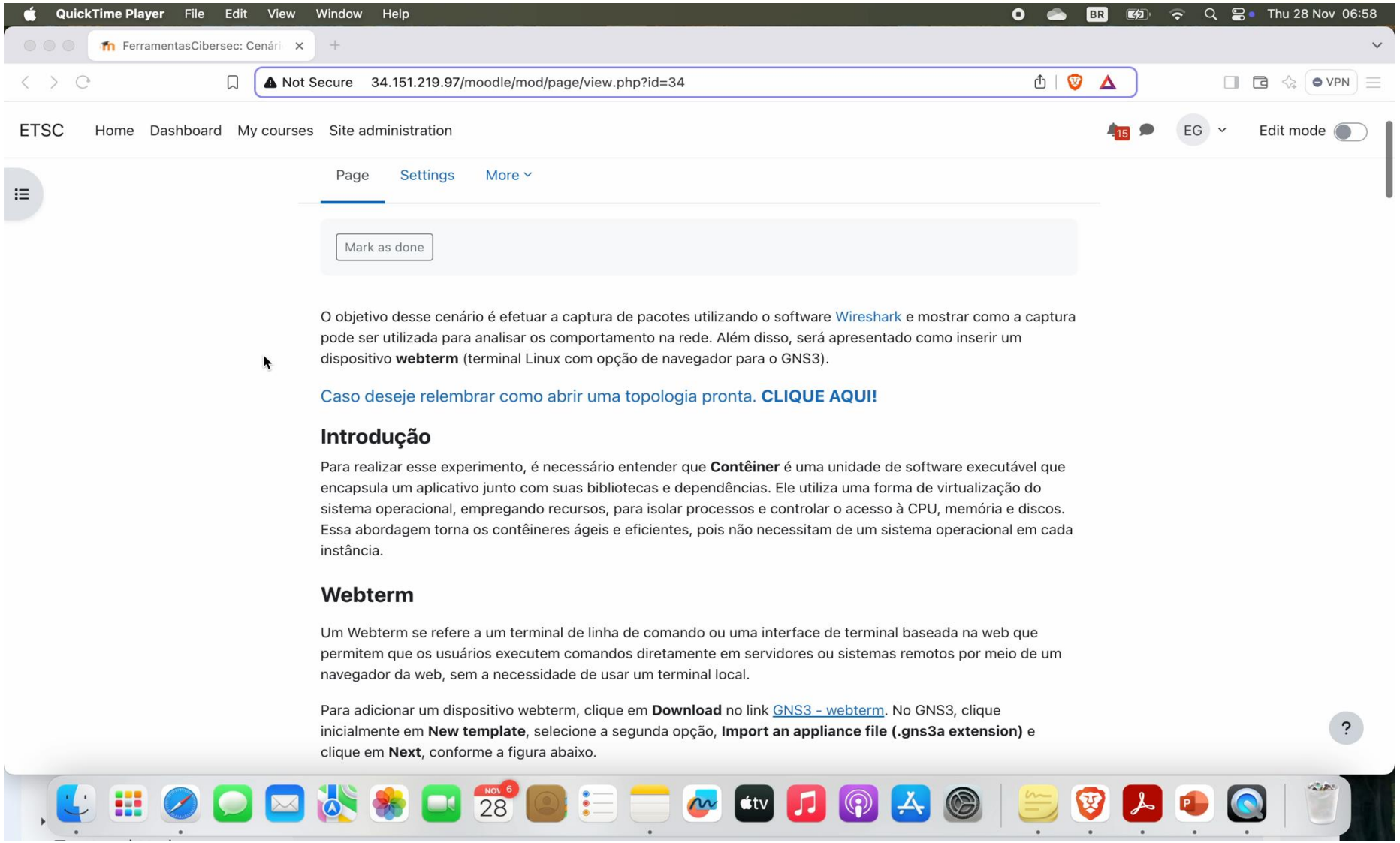
Cenário: tarefas para experimentação; 

Cursos:

- **Ferramentas: 16 cenários;** 1 2 ... 16
- **Red Team: 18 cenários:** 1 2 ... 18
- **Blue Team: 11 cenários:** 1 2 ... 11

Instrutor escolhe ferramentas de acordo com o público;

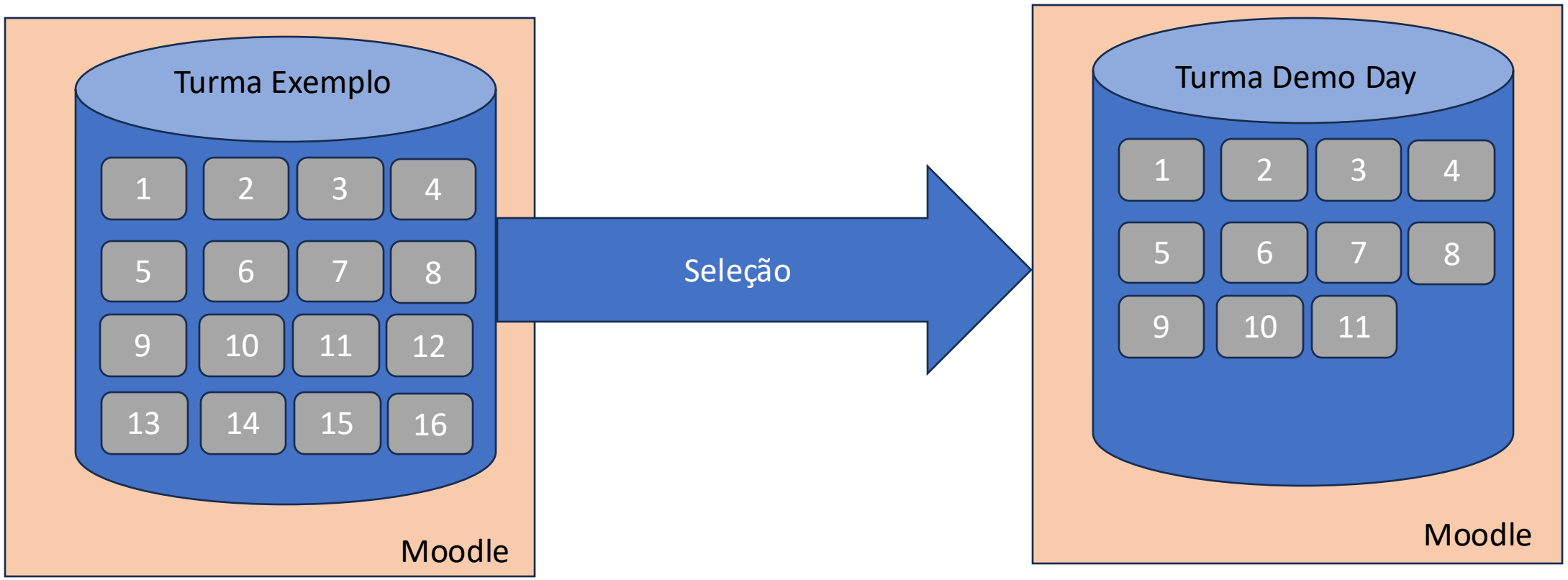
Definições


QuickTime Player File Edit View Window Help
Thu 28 Nov 06:58
FerramentasCibersec: Cenári
Not Secure 34.151.219.97/moodle/mod/page/view.php?id=34
VPN
ETSC Home Dashboard My courses Site administration
EG
Edit mode
Page Settings More
Mark as done
O objetivo desse cenário é efetuar a captura de pacotes utilizando o software Wireshark e mostrar como a captura pode ser utilizada para analisar os comportamento na rede. Além disso, será apresentado como inserir um dispositivo webterm (terminal Linux com opção de navegador para o GNS3).
Caso deseje relembrar como abrir uma topologia pronta. CLIQUE AQUI!
Introdução
Para realizar esse experimento, é necessário entender que Contêiner é uma unidade de software executável que encapsula um aplicativo junto com suas bibliotecas e dependências. Ele utiliza uma forma de virtualização do sistema operacional, empregando recursos, para isolar processos e controlar o acesso à CPU, memória e discos. Essa abordagem torna os contêineres ágeis e eficientes, pois não necessitam de um sistema operacional em cada instância.
Webterm
Um Webterm se refere a um terminal de linha de comando ou uma interface de terminal baseada na web que permitem que os usuários executem comandos diretamente em servidores ou sistemas remotos por meio de um navegador da web, sem a necessidade de usar um terminal local.
Para adicionar um dispositivo webterm, clique em Download no link GNS3 - webterm. No GNS3, clique inicialmente em New template, selecione a segunda opção, Import an appliance file (.gns3a extension) e clique em Next, conforme a figura abaixo.

Exemplo

Ferramentas:

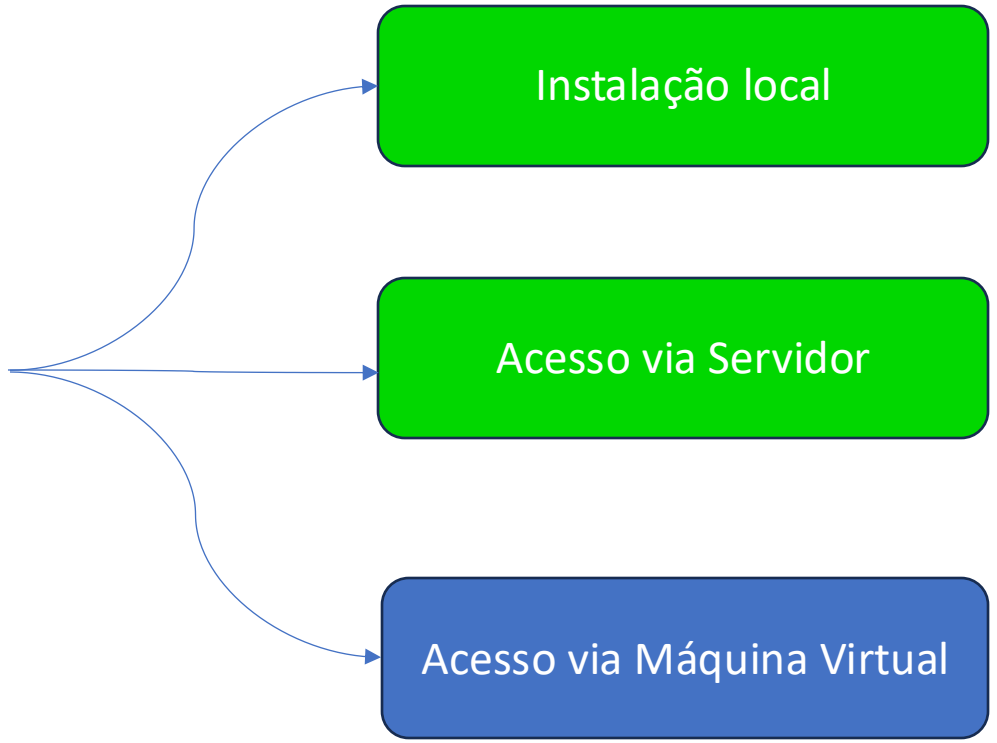
- **Iniciante:** sem conhecimento básico de redes ou Linux ➔ Ferramentas (essencial): 1 ao 11, Red Team e Blue Team;



Graphical Network Simulator 3 (GNS3):

- **Código livre;**
- **Uso de contêiner;**

Possibilidades



Recomendação

Acesso via Máquina Virtual

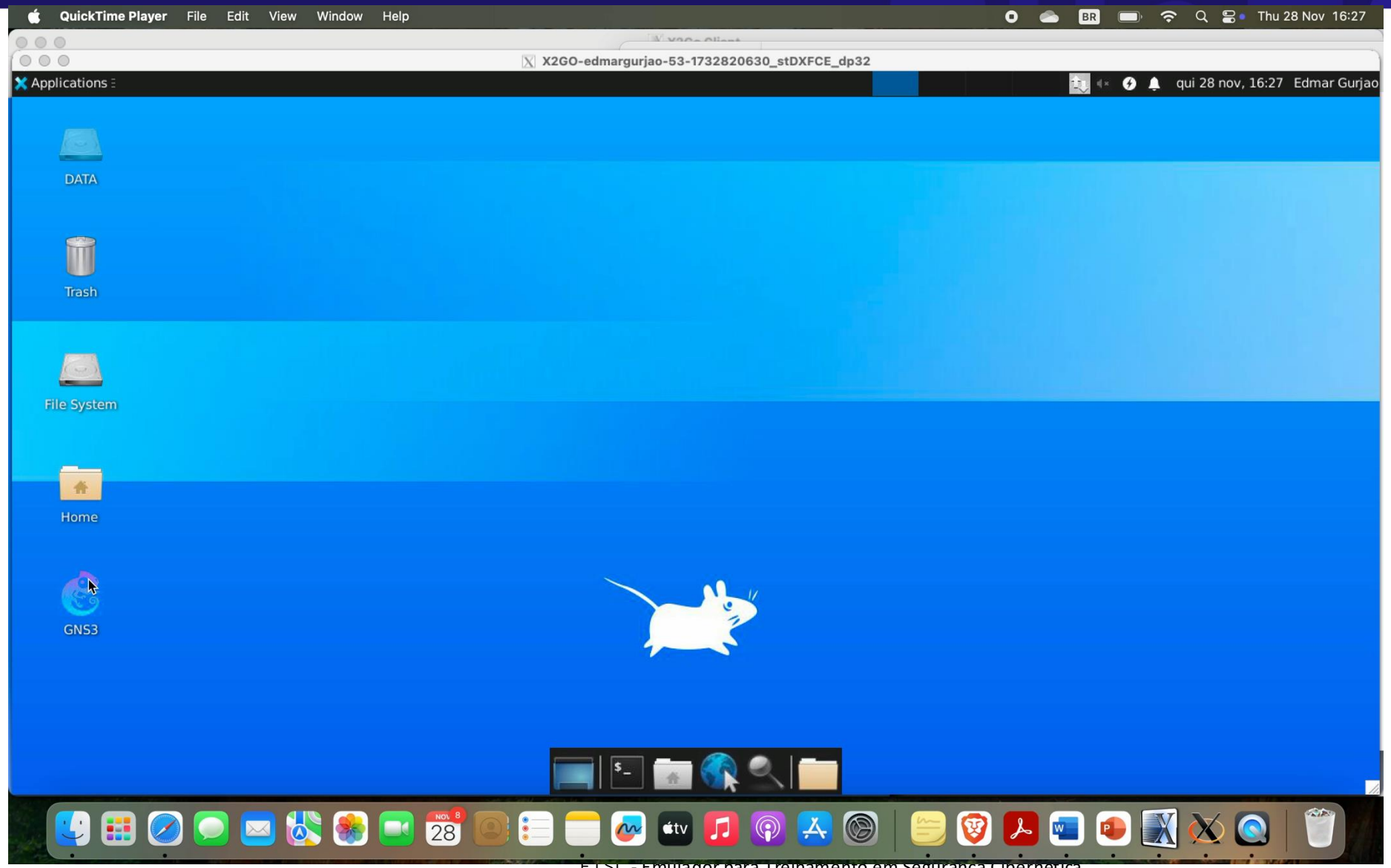
Vantagens:

- **Sem necessidade de instalação local;**
- **Sem problemas de escalabilidade, como no caso do servidor;**

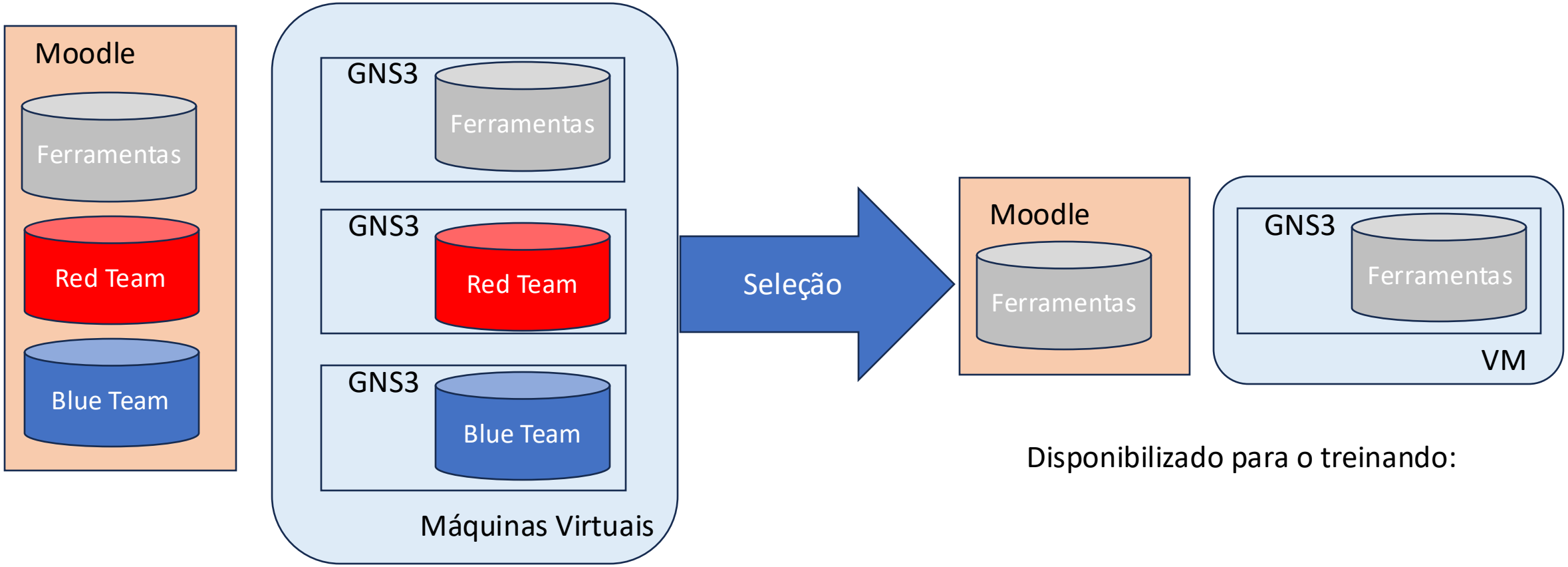
Problema:

- **Máquina com simulador 6GB e cenários para download;**

Recomendação



Plataforma



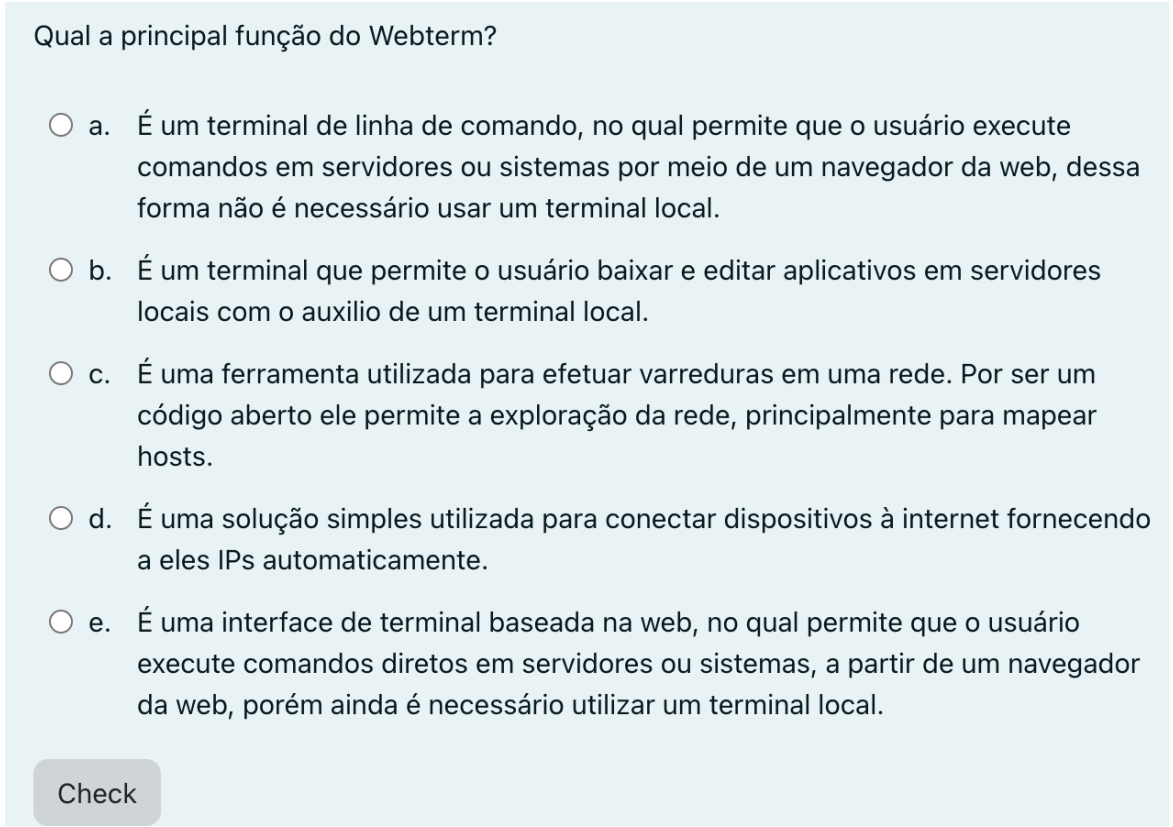
Disponibilizado para o treinando:

Avaliação de Aprendizagem

Formulários Pré e Pós Cursos

- Mesmas questões (ordem aleatória)

Quiz em todos os cenários

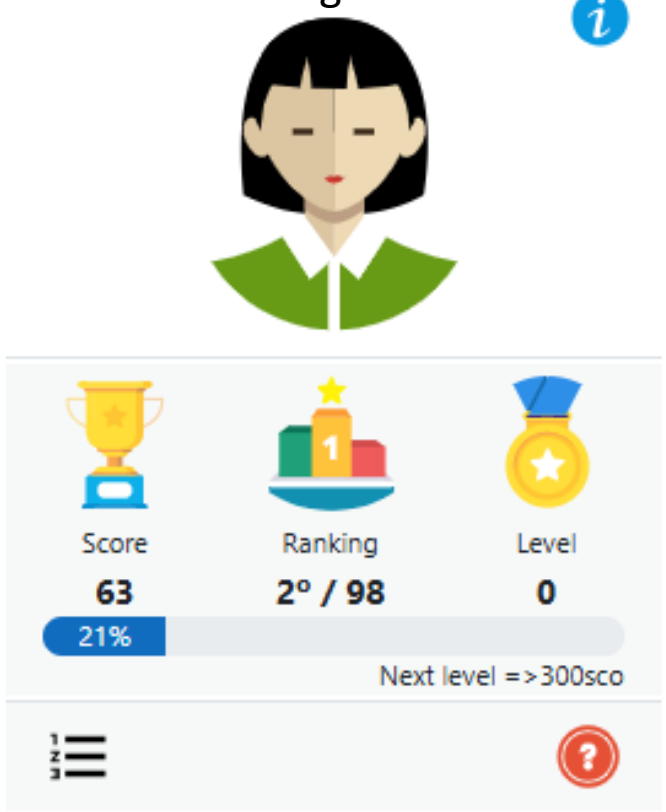


- Mesmas questões (ordem aleatória)
- Mesmas questões (ordem aleatória)
- Mesmas questões (ordem aleatória)
- Mesmas questões (ordem aleatória)

Gamificação: estudantes podem ser classificados

Game

Block Game – Pugin Moodle



Cursos ministrados

– Polícia Civil da Paraíba:

- Ferramentas;
- 30 alunos com conhecimento em redes de computadores;
- Laboratório da ACADEPOL.

- **Alunos de Graduação em Engenharia Elétrica**
  - Ferramentas;
  - 12 alunos sem conhecimentos prévios em redes de computadores;
  - Laboratório da UFCG.

Cursos ministrados

– Polícia Militar da Paraíba:

- Ferramentas, Red Team, Blue Team;
- 25 profissionais
- Híbrido.

- **Alunos de Graduação em Ciências da Computação**
  - Ferramentas;
  - 20 alunos com conhecimentos prévios em redes de computadores;
  - Laboratório da UFCG.
  - Todos os cenários realizados em um dia (8 horas de aula)

Próximos Passos

- **Módulo Forense;**
- **Integração Moodle e GNS3: cenário no Moodle recebe parâmetros do GNS3;**
- **Implementação do Copiloto;**
- **Uso de metodologia Confidence-Based Assessment *para avaliação do aprendizado;***

ETSC – Emulador para Treinamento em Segurança Cibernética
https://cyberedu.com.br/

Obrigado!

Edmar C. Gurjão

ecg@dee.ufcg.edu.br