

## 1. Introdução e Objetivos (Primeiro tópico do Slide da aula)

**Objetivo Geral:** Capacitar os alunos a construir e configurar um ambiente de laboratório seguro para a prática de conceitos de cibersegurança.

### Objetivos Específicos:

- Criar e configurar duas VMs por aluno: uma VM de servidor web e outra VM apenas com o Debian instalado.
- Configurar 5 VLANs no roteador para simular diferentes segmentos de rede.
- Desenvolver um plano de cibersegurança cobrindo as fases de Identificação, Proteção, Detecção, Resposta e Recuperação.

## 2. Configuração do Roteador (**Será entregue configurado**)

### Teoria:

- Conceitos de VLAN e sua importância na segmentação de redes e na segurança.
- Princípios básicos de roteamento e isolamento de rede.

### Prática:

- Configuração de 5 VLANs no roteador para separar as diferentes máquinas virtuais e simular um ambiente de rede realístico.
- Definição de regras básicas de acesso entre as VLANs.

## 3. Configuração do Computador do Aluno

### Criação das VMs:

- **VM de Servidor Web:**
  - ✓ Instalação do Debian e configuração de um servidor web (Apache, Nginx ou outro).
  - ✓ Implementação de medidas básicas de segurança para proteger o servidor web.
- **VM Debian Padrão:**
  - ✓ Instalação do Debian com configuração padrão para simular um cliente ou uma estação de trabalho comum.

### Atividades Práticas:

- Instalação e configuração do VirtualBox ou outro software de virtualização.
- Criação e configuração das VMs conforme os objetivos específicos.
- Testes de conectividade e acesso básico entre as VMs e o acesso à internet.

## 4. Desenvolvimento do Plano de Cibersegurança

### Teoria e Prática:

- **Identificação:** Análise e listagem de ativos, avaliação de impacto e vulnerabilidades.
- **Proteção:** Configuração de auditorias, gerenciamento de acesso e backups.

- **Detecção:** Implementação de ferramentas de detecção de intrusão e análise de logs.
- **Resposta:** Desenvolvimento de um plano de resposta a incidentes.
- **Recuperação:** Criação de um plano de recuperação de desastres.

## **5. Atividades Práticas Complementares**

- Simulações de ataques e defesas em um ambiente controlado.
- Uso de ferramentas de auditoria de segurança para identificar vulnerabilidades nas VMs.
- Práticas de backup e recuperação de dados.

## **6. Avaliação e Feedback**

### **Avaliação:**

- Apresentação do plano de cibersegurança elaborado.
- Demonstração prática das configurações de segurança implementadas nas VMs.

### **Feedback:**

- Discussão sobre as soluções adotadas pelos alunos.
- Sugestões de melhorias e pontos de atenção.

## **Material de Apoio e Referências**

- Documentação oficial do Debian para instalação e configuração.
- Guias de segurança para servidores web.
- Material sobre VLANs e configuração de roteadores.