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.

7. Ferramentas do Kali Linux para a Execução da Atividade

1. **Nmap - Objetivo: Identificação e Mapeamento de Rede**
   - ✓ **Descrição:** Nmap (Network Mapper) é uma ferramenta de código aberto usada para explorar redes e realizar auditorias de segurança. Ela permite aos alunos identificar dispositivos ativos na rede, serviços rodando, sistemas operacionais instalados, e possíveis pontos vulneráveis.
2. **Wireshark - Objetivo: Detecção e Análise de Tráfego de Rede**
   - ✓ **Descrição:** Wireshark é um analisador de protocolo de rede que permite capturar e interativamente examinar o tráfego de uma rede. É essencial para entender o comportamento da rede e detectar atividades suspeitas.
3. **Metasploit Framework - Objetivo: Teste de Penetração e Desenvolvimento de Resposta a Incidentes**
   - ✓ **Descrição:** Metasploit é uma das ferramentas mais populares para desenvolvimento e execução de exploits contra sistemas remotos. Auxilia na identificação de vulnerabilidades e na preparação dos alunos para desenvolver estratégias eficazes de resposta a incidentes.
4. **Burp Suite - Objetivo: Teste de Segurança de Aplicações Web**

- ✓ **Descrição:** Burp Suite é um conjunto de ferramentas para a realização de testes de segurança em aplicações web. Permite aos alunos identificar vulnerabilidades em aplicações web que estão rodando na VM de servidor.

5. **Aircrack-ng - Objetivo: Testes de Segurança em Redes Wi-Fi**
   - ✓ **Descrição:** Aircrack-ng é um conjunto completo de ferramentas para avaliar a segurança de redes Wi-Fi. Através dela, é possível entender e testar a segurança das comunicações sem fio.
6. **Sqlmap - Objetivo: Automatização de Detecção e Exploração de Vulnerabilidades SQL Injection**
   - ✓ **Descrição:** Sqlmap é uma ferramenta de teste de penetração que automatiza o processo de detecção e exploração de vulnerabilidades de injeção SQL em aplicações web. Essencial para a fase de proteção, identificando falhas críticas em aplicações web.
7. **John the Ripper - Objetivo: Teste de Força-Bruta em Senhas**
   - ✓ **Descrição:** John the Ripper é uma ferramenta de quebra de senha rápida, usada para testar a força das senhas usadas nos sistemas operacionais das VMs. Contribui para a fase de proteção ao reforçar a necessidade de senhas fortes.
8. **Gobuster - Objetivo: Enumeração de Diretórios e Subdomínios Web**
   - ✓ **Descrição:** Gobuster é uma ferramenta usada para enumeração de diretórios e subdomínios em websites. Ajuda a identificar recursos ocultos ou não documentados em aplicações web.