Atividade 1:

Técnicas de ataque utilizadas:

- **Phishing**: O atacante usou uma isca para enganar o funcionário, fazendo-o acreditar que estava interagindo com uma recrutadora legítima. O ataque foi disfarçado de uma "pesquisa", mas na realidade era um malware.
- **Malware**: O “formulário de pesquisa” era, na verdade, um malware que foi executado no computador do funcionário, dando acesso remoto ao sistema da empresa.

Camadas de segurança vulneráveis:

1. **Camada técnica**: A vulnerabilidade foi na segurança do computador corporativo, permitindo que o malware fosse executado e desse acesso remoto ao sistema da empresa.
2. **Camada humana**: O funcionário foi enganado por uma tática de manipulação social (social engineering). A falta de conscientização e treinamento sobre como identificar tentativas de phishing e malware contribuiu para o sucesso do ataque.

Três ações de prevenção:

1. **Treinamento e conscientização**: Realizar treinamentos regulares sobre segurança cibernética para funcionários, abordando como identificar tentativas de phishing e os riscos de clicar em links suspeitos.
2. **Implementação de filtros de e-mails e links**: Utilizar sistemas de filtragem de e-mails e links que detectem e bloqueiem conteúdos maliciosos, além de verificar a autenticidade de mensagens recebidas por plataformas como WhatsApp.
3. **Segurança avançada nos dispositivos corporativos**: Garantir que todos os dispositivos corporativos possuam antivírus e firewalls atualizados e que o acesso remoto seja restrito e monitorado para evitar acessos não autorizados.

Atividade 2:

Explicação dos ataques:

- **SQL Injection**: O SQL Injection é uma técnica de ataque em que o atacante insere comandos SQL maliciosos em campos de entrada de um aplicativo (como formulários de login ou busca) para manipular ou acessar dados do

banco de dados de forma não autorizada. O objetivo é executar comandos SQL no banco de dados, podendo exfiltrar dados sensíveis, modificar informações ou até mesmo destruir o banco de dados.

- **DDoS (Distributed Denial of Service):** Um ataque DDoS ocorre quando um grande número de dispositivos (geralmente uma rede de computadores comprometidos) é usado para enviar uma quantidade massiva de tráfego para um servidor ou rede, sobrecarregando os recursos e tornando-os inacessíveis para os usuários legítimos. O objetivo é derrubar o serviço ou deixá-lo fora do ar, dificultando ou impedindo o acesso.

Consulta à IA sobre SQL Injection:

Pesquisei e a resposta obtida foi: *"Para evitar ataques de SQL Injection em aplicações modernas, recomenda-se o uso de prepared statements (declarações preparadas) com parâmetros, validação rigorosa de entradas, e o uso de ORM (Object-Relational Mapping) para abstrair a interação direta com o banco de dados."*

Comparação:

- **Semelhanças**:
    1. Ambos sugerem o uso de prepared statements para evitar a injeção de código malicioso.
    2. A validação de entradas é mencionada como uma prática essencial para prevenir SQL Injection.
- **Diferença**:
    1. A resposta consultada menciona o uso de ORM (Object-Relational Mapping) como uma forma de abstrair a interação com o banco de dados, o que não é abordado diretamente no item "Mergulhando no Tema".