# Exercícios Redes Seguras – Arquitetura

## 1. Quais são os Ativos de rede identificados na arquitetura? (mínimo 5, com funções detalhadas)

Ativos de rede identificados:  
  
1. Firewall Externo  
- Função: Controla o tráfego que entra e sai da rede da empresa vinda da internet. Filtra conexões suspeitas antes de alcançarem o roteador interno.  
- Importância: Primeira linha de defesa contra ataques externos.  
  
2. Roteador  
- Função: Direciona o tráfego de rede entre diferentes redes (internet ↔ rede interna). Trabalha junto ao firewall externo para garantir que só o tráfego permitido circule.  
- Importância: Faz o roteamento de pacotes, verificando os destinos e encaminhando-os de forma segura.  
  
3. Firewall Interno + ADS (Sistema de Detecção de Ataques)  
- Função: Monitora o tráfego interno da rede e identifica tentativas de invasão. O ADS detecta padrões de ataque como tentativas de exploração e movimentação lateral na rede.  
- Importância: Segunda linha de defesa, evita que um ataque interno se propague.  
  
4. Switches / Interruptores de Rede  
- Função: Fazem a conexão física entre os diversos equipamentos (servidores e estações de trabalho), distribuindo o tráfego interno da empresa.  
- Importância: Permitem segmentação de rede, controle de VLANs e podem ser usados para aplicar políticas de segurança.  
  
5. Servidor de Diretório (Alvo 2)  
- Função: Gerencia autenticação e autorização de usuários, centralizando contas de rede, permissões e políticas de grupo (ex.: Active Directory).  
- Importância: Controla quem pode acessar os demais ativos da rede.  
  
6. Servidores (Base de Dados, FTP, Correio, Ficheiro - Alvos 1, 3 e outros)  
- Função: Hospedam dados, serviços de e-mail, compartilhamento de arquivos e banco de dados da empresa.  
- Importância: São os principais alvos de ataques, pois contêm dados sensíveis.  
  
7. Honeypot Interno  
- Função: Simula um servidor vulnerável para atrair possíveis invasores e detectar comportamentos maliciosos.  
- Importância: Serve como armadilha para atrasar, desviar e estudar ataques.

## 2. Qual técnica o Hacker está utilizando para fazer o ataque?

Técnica: Engenharia Social - Phishing  
  
Como funciona:  
O hacker está enviando mensagens falsas para colaboradores em trabalho remoto (veja a seta azul saindo do hacker para o trabalho remoto). Provavelmente, ele está enviando e-mails ou mensagens com links maliciosos ou pedindo informações de acesso.  
  
Justificativa no cenário:  
- A rede da empresa só é acessível via VPN, então o hacker precisa das credenciais de um colaborador para entrar.  
- O ataque de engenharia social (phishing) é a melhor forma de conseguir essas credenciais sem precisar atacar o perímetro físico da rede.

## 3. Quantos colaboradores precisam preencher o formulário falso para o Hacker conseguir acessar?

Resposta: Apenas 1 colaborador.  
  
Justificativa:  
Basta um único colaborador fornecer suas credenciais (login e senha) para que o hacker ganhe acesso VPN à rede interna da empresa.

## 4. Outras técnicas que o Hacker poderia utilizar e os desafios:

| Técnica Alternativa | Descrição | Desafios Enfrentados |  
  
| Brute Force contra a VPN | Tentativas automatizadas de adivinhar senhas da VPN | Limite de tentativas + bloqueios automáticos + autenticação multifator |  
| Ataques de Malware/Keylogger | Infectar o PC do colaborador com um malware que captura senhas | Sistemas de antivírus, firewalls pessoais e atualizações de segurança |  
| Ataque Man-in-the-Middle (MITM) | Interceptar a comunicação entre o colaborador e a VPN | Uso de criptografia (SSL/TLS), VPNs seguras e redes protegidas |  
| Exploração de Vulnerabilidades em Serviços Expostos (ex.: FTP) | Tentar explorar falhas de configuração nos serviços acessíveis | Firewalls, IDS/IPS, patches de segurança atualizados |

## 5. Melhorias de segurança para mitigar a invasão:

| Melhorias Sugeridas | Justificativa |  
  
| Implementação de Autenticação Multifator (MFA) na VPN | Mesmo que o hacker consiga a senha, ele precisará de um segundo fator para acessar |  
| Campanhas de Conscientização contra Phishing | Treinar os funcionários para reconhecerem e evitarem e-mails falsos |  
| Monitoramento de Logs de VPN e Atividades Anômalas | Detectar acessos suspeitos fora de horário ou de IPs não usuais |  
| Segmentação de Rede e Limitação de Acessos (Least Privilege) | Se o hacker conseguir acesso, ele terá acesso apenas ao mínimo necessário, dificultando o movimento lateral |

## 6. O que poderia ser implementado em cada Alvo para garantir a segurança?

| Alvo | Ações para Segurança | Riscos caso não seja feito |  
|---|---|---|  
| Alvo 1 - Base de Dados | - Uso de criptografia de dados\n- Controle de acesso por perfil\n- Auditoria de logs de acesso | Vazamento de dados sensíveis (clientes, contratos, etc.) |  
| Alvo 2 - Servidor de Diretório | - Autenticação forte (MFA para administradores)\n- Monitoramento de alterações de conta\n- Política de senha robusta | Controle total da rede pelo hacker caso ele comprometa este servidor |  
| Alvo 3 - Servidor de Correio | - Filtros anti-spam e anti-phishing\n- Monitoramento de envio de e-mails em massa\n- Proteção contra ataques de spoofing | Uso do servidor para envio de spam ou como vetor para novos ataques |  
| Alvo 4 - Switch interno | - Controle de portas (Port Security)\n- Monitoramento de tráfego anômalo\n- VLANs para segmentação | Ataques internos como sniffing ou envenenamento de ARP se o hacker tiver acesso físico ou lógico |