Introdução à Segurança Defensiva - TryHackMe

Resumo: Conceitos Básicos da Segurança Defensiva

A segurança ofensiva busca explorar vulnerabilidades para fortalecer sistemas. Já a **segurança defensiva** tem como foco:

- **Prevenir intrusões**
- **Detectar e responder a ataques**

As **Blue Teams** atuam nessa área, sendo responsáveis por proteger os sistemas antes, durante e após tentativas de invasão.

Principais Tarefas da Segurança Defensiva

- **Conscientização dos usuários**: Treinar usuários para evitar ataques direcionados.
- **Gestão de ativos**: Conhecer os sistemas e dispositivos que precisam ser protegidos.
- **Atualizações e correções**: Manter todos os sistemas atualizados contra vulnerabilidades conhecidas.
- **Dispositivos de prevenção**: Firewalls e sistemas de prevenção de intrusão (IPS) bloqueiam tráfego malicioso.
- **Monitoramento e registro**: Detectar atividades suspeitas por meio de logs e ferramentas de monitoramento.

Áreas Específicas da Segurança Defensiva

1. Centro de Operações de Segurança (SOC)

Um SOC é uma equipe especializada em monitorar redes e sistemas em busca de atividades maliciosas. Principais pontos:

- **Vulnerabilidades**: Detectar e corrigir falhas antes que sejam exploradas.
- **Violações de políticas**: Monitorar e identificar ações contrárias às diretrizes de segurança.
- **Atividades não autorizadas**: Impedir o uso indevido de credenciais ou sistemas.
- **Intrusões**: Detectar rapidamente qualquer tentativa de invasão.

2. Inteligência de Ameaças (Threat Intelligence)

Consiste em **coletar, processar e analisar dados** para entender o comportamento e os objetivos dos atacantes. Isso permite:

- **Previsão de ataques**
- **Preparação de defesas específicas**
- **Identificação de adversários (ex: grupos de ransomware, exércitos cibernéticos)**

DFIR: Resposta a Incidentes e Análise Forense Digital

1. Forense Digital

Investiga crimes cibernéticos com base em evidências digitais:

- **Sistema de arquivos**: Descoberta de arquivos apagados, programas instalados etc.
- **Memória do sistema**: Análise de malwares que operam apenas em RAM.
- **Logs do sistema e da rede**: Rastreiam atividades suspeitas, mesmo após tentativas de ocultação.

2. Resposta a Incidentes

Processo estruturado para lidar com ataques:

1. **Preparação**: Equipe treinada e planos definidos.
2. **Detecção e Análise**: Identificação e avaliação da gravidade do incidente.
3. **Conter, Erradicar e Recuperar**: Isolamento, eliminação da ameaça e recuperação do sistema.
4. **Pós-incidente**: Geração de relatórios e lições aprendidas.

Análise de Malware

Tipos comuns de malware:

- **Vírus**: Alteram e corrompem arquivos.
- **Cavalo de Troia (Trojan)**: Disfarçados de programas úteis, mas com funções maliciosas ocultas.
- **Ransomware**: Criptografa arquivos e exige pagamento para liberar o acesso.

Técnicas de análise:

- **Estática**: Análise do código sem executá-lo.
- **Dinâmica**: Execução em ambiente controlado para observar o comportamento.

Exemplo Prático: Atuação como Analista de SOC

Imagine que você está protegendo um banco e monitora alertas usando um sistema SIEM. Nem todo alerta é malicioso — alguns podem ser simples erros de login ou conexões suspeitas.

Desafio Prático (TryHackMe):

Acesse o site simulado, siga os passos, investigue os eventos e encontre a "flag" no formato `THM{PALAVRAS_ALEATÓRIAS}`.

Próximos Passos

Você conheceu:

- SOC
- Threat Intelligence
- DFIR
- Análise de Malware