1.Introdução

Cibersegurança é uma constante luta entre *white hats* e *black hats*. Conforme o nível de ameaça cibernético aumenta, aumenta também a necessidade de serviços mais especializados que permitam empresas a se prepararem contra ataques reais da melhor maneira possível.

2.Avaliação de vulnerabilidades e limites de testes de penetração

Este é o mais simples e seu principal objetivo é identificar a maior quantidade de vulnerabilidades possíveis na maior quantidade de sistemas possíveis de uma determinada rede. Para simplificar, uma **avaliação de vulnerabilidades** tem como foco realizar scans em hosts para encontrar vulnerabilidades como entidades individuais para que então, os problemas de segurança possam ser identificados e efetivamente tornados seguros. A maioria do trabalho pode ser realizada com ferramentas automáticas sem a necessidade de muito conhecimento técnico.

Os testes de penetração aumentam as avaliações de vulnerabilidade ao permitir que o pentester explore o impacto de um invasor na rede geral, realizando etapas adicionais que incluem:

- Tentativa de explorar vulnerabilidades encontradas em cada sistema. Isto é importante pois uma vulnerabilidade pode existir em um sistema, mas controles postos em prática podem prevenir efetivamente esta exploração, permitindo verificar se sistemas podem detectar vulnerabilidades comprometedoras dado um host
- Conduzir tarefas de pós-exploração com o host, permitindo extrair informações úteis que podem ser usadas para contornar outros hosts que não estavam acessíveis previamente

Os testes de penetração podem começar escaneando vulnerabilidades como uma avaliação de vulnerabilidade regular, mas fornecem mais informações sobre como um invasor pode desencadear vulnerabilidades para atingir objetivos específicos. Embora seu foco permaneça na identificação de vulnerabilidades e no estabelecimento de medidas para proteger a rede, ele também considera a rede como um ecossistema inteiro e como um invasor pode lucrar com as interações entre seus componentes

Ao analisar como um invasor pode se movimentar em nossa rede, também obtemos uma visão básica sobre possíveis desvios de medidas de segurança e nossa capacidade de detectar um agente de ameaça real até certo ponto, limitada porque o escopo de um teste de penetração geralmente é extenso e os testadores de penetração não se importam muito em fazer barulho ou gerar muitos alertas em dispositivos de segurança, já que as restrições de tempo em tais projetos geralmente exigem que verifiquemos a rede em um curto espaço de tempo.

Como consequência, alguns aspectos do teste de penetração podem ser diferentes de um ataque real:

- **Testes de penetração são "barulhentos":** Normalmente, os pentesters não se esforçam muito para tentar passar despercebidos. Ao contrário dos invasores reais, eles não se importam em ser fáceis de detectar, pois foram contratados para encontrar o máximo de vulnerabilidades possível em tantos hosts quanto possível
- **Relaxamento de mecanismos de segurança:** Ao fazer um teste de penetração regular, alguns mecanismos de segurança podem ser temporariamente desabilitados ou relaxados para a equipe de pentesting em favor da eficiência. Embora isso possa parecer contra-intuitivo, é essencial lembrar que os pentesters têm tempo limitado para verificar a rede. Portanto, geralmente é desejável não desperdiçar seu tempo procurando maneiras exóticas de contornar IDS/IPS, WAF, engano de intrusão ou outras medidas de segurança, mas sim focar na revisão de infraestrutura tecnológica crítica para vulnerabilidades
- **Vetores de ataque não técnicos podem ser negligenciados:** Ataques baseados em engenharia social ou intrusões físicas geralmente não são incluídos no que é testado

Os verdadeiros atacantes não seguem um código ético e são, em sua maioria, irrestritos em suas ações. Hoje em dia, os atores de ameaças mais proeminentes são conhecidos como **Advanced Persistent Threats** (APT), que são grupos altamente qualificados de atacantes, geralmente patrocinados por nações ou grupos criminosos organizados. Eles têm como alvo principal infraestrutura crítica, organizações financeiras e instituições governamentais. Eles são chamados de persistentes porque as operações desses grupos podem permanecer sem serem detectadas em redes comprometidas por longos períodos.

3.Compromissos de um Red team

Para acompanhar as ameaças emergentes, os engajamentos da equipe vermelha foram projetados para mudar o foco de testes de penetração regulares para um processo que nos permite ver claramente as capacidades da nossa equipe defensiva em *detectar* e *responder* a um agente de ameaça real.

Em exercícios militares, um grupo assumiria o papel de uma *red team* para simular técnicas de ataque para testar as capacidades de reação de uma equipe de defesa, geralmente conhecida como *blue team*, contra estratégias adversárias conhecidas .Os engajamentos da equipe vermelha consistem em emular as **Táticas**, **Técnicas e Procedimentos** (TTPs) de um agente de ameaça real para que possamos medir o quão bem um *blue team* responde a eles e, finalmente, melhorar quaisquer controles de segurança em vigor.

Cada engajamento da equipe vermelha começará definindo objetivos claros, frequentemente referenciados como *flags*, variando de comprometer um determinado host crítico a roubar algumas informações confidenciais do alvo. Normalmente, o *blue team* não será informado de tais exercícios para evitar introduzir quaisquer vieses em sua análise. O *red team* fará tudo o que puder para atingir os objetivos, permanecendo sem ser detectada e evitando quaisquer mecanismos de segurança existentes, como firewalls, antivírus, EDR, IPS e outros.

Observe como em um engajamento do *red team*, nem todos os hosts em uma rede serão verificados quanto a vulnerabilidades. Um invasor real só precisaria encontrar um único caminho para seu objetivo e não está interessado em executar varreduras ruidosas que o *blue team* pudesse detectar.

Os engajamentos do *red team* também melhoram em testes de penetração regulares ao considerar diversas superfícies de ataque:

- **Infraestrutura técnica:** Como em um teste de penetração regular, uma equipe vermelha tentará descobrir vulnerabilidades técnicas, com uma ênfase muito maior em furtividade e evasão
- **Engenharia social:** Atacar pessoas por meio de campanhas de phishing, ligações telefônicas ou mídias sociais para induzi-las a revelar informações que deveriam ser privadas
- **Intrusão física:** Usando técnicas como arrombamento, clonagem RFID, exploração de fraquezas em dispositivos de controle de acesso eletrônico para acessar áreas restritas de instalações

Dependendo dos recursos disponíveis, o exercício da equipe vermelha pode ser executado de várias maneiras:

- **Vulnerabilidade assumida:** Comece assumindo que o invasor já obteve controle sobre alguns ativos e tente atingir os objetivos a partir daí. Como exemplo, a equipe vermelha poderia receber acesso às credenciais de algum usuário ou até mesmo a uma estação de trabalho na rede interna.
- **Envolvimento total:** simule o fluxo de trabalho completo de um invasor, desde o comprometimento inicial até que os objetivos finais sejam alcançados
- **Exercício de mesa:** Uma simulação sobre a mesa onde cenários são discutidos entre as equipes vermelha e azul para avaliar como elas teoricamente responderiam a certas ameaças. Ideal para situações em que fazer simulações ao vivo pode ser complicado

4.Times e funções de engajamento

Há vários fatores e pessoas envolvidas em um engajamento de *red team*. Todos terão sua mentalidade e metodologia para abordar o pessoal de engajamento; no entanto, cada engajamento pode ser dividido em três equipes ou células.

4.1 Red cell

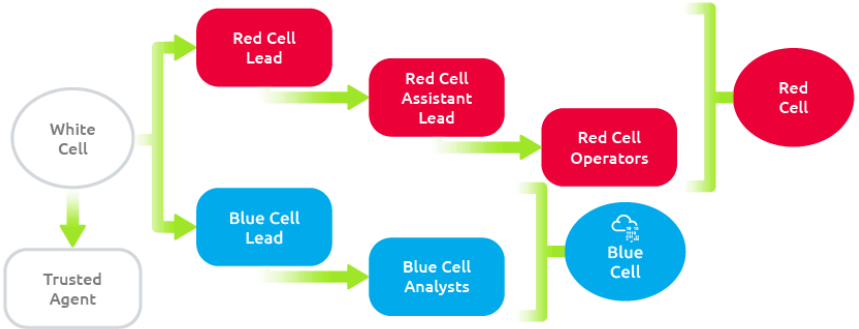
Uma **red cell** é o comportamento que compõe a parte ofensiva de um engajamento de um **red team** que simula as respostas estratégicas e táticas de um determinado alvo

4.2 Blue cell

Uma **blue cell** é o lado oposto do **red cell**. Isso inclui todos os componentes que defendem uma rede alvo. A **blue cell** é normalmente composta por membros de um **blue team**, defensores, equipe interna e gerenciamento de uma organização

4.3 White cell

Serve como árbitro entre as atividades de ambas as células durante um compromisso. Controla o ambiente/rede de engajamento, monitora a adesão ao ROE, coordena as atividades necessárias para atingir as metas de engajamento. Correlaciona atividades dos **red cells** com ações defensivas e garante que o envolvimento seja conduzido sem preconceitos para nenhum dos lados



4.4 Red team lead

Planeja e organiza compromissos em alto nível. Delegados, líder assistente e atribuições de envolvimento de operadores

4.5 Red team assistant lead

Auxilia o líder **red team** na supervisão de operações e operadores de engajamento. Também pode ajudar na redação de planos de trabalho e documentação, se necessário

4.6 Red team operator

Executa tarefas delegadas pelos líderes da equipe. Interpreta e analisa os planos de engajamento dos líderes da equipe

5.Estruturas de engajamento

Uma função essencial da equipe vermelha é a emulação do adversário. Embora não seja obrigatória, é comumente usada para avaliar o que um adversário real faria em um ambiente usando suas ferramentas e metodologias. O *red team pode* usar várias *cyber kill chains* para resumir e avaliar as etapas e procedimentos de um engajamento. Below is a small list of standard cyber kill chains:

- **Lockheed Martin Cyber Kill Chain**
- **Unified Kill Chain**
- **Varonis Cyber Kill Chain**
- **Active Directory Attack Cycle**
- **MITRE ATT&CK Framework**

Os componentes da cadeia de eliminação estão detalhados na tabela abaixo:

Técnica	Propósito	Exemplos
Reconnaissance	Obter informações do alvo	Busca de e-mails, OSINT
Weaponization	Combinar os objetivos com um exploit	Exploit com backdoor, documentos maliciosos
Delivery	Como o exploit vai ser enviado ao alvo	E-mail, web, USB
Exploitation	Explora o sistema alvo para executar código	MS17-010, Zero-logon, etc
Installation	Instalar malware e outras ferramentas	Mimikatz, Rubeus
Command and Control (C2)	Controle do alvo comprometido estabelecendo uma central de comandos	Empire, Cobalt Strike
Actions on Objectives	Qualquer objetivo final	Conti, LockBit2.0