1.Introdução

Engajamentos podem ser complexos e burocráticos. A chave para o sucesso de um é ter bem definido os objetivos ou metas. Os objetivos do cliente devem ser discutidos entre o cliente e a equipe vermelha para criar um entendimento mútuo entre ambas as partes sobre o que é esperado e fornecido.

Objetivos definidos são a base para o restante da documentação e planejamento do engajamento. Sem objetivos e expectativas claros e concretos, você está se preparando para uma campanha muito desestruturada e não planejada. Os objetivos definem o tom para o resto do engajamento. As especificidades da abordagem dependerão do envolvimento definido caso a caso pelos objetivos do cliente.

Os objetivos do cliente apenas estabelecem uma definição básica dos objetivos do cliente para o engajamento. Os planos de engajamento específicos expandirão os objetivos do cliente e determinarão as especificidades do engajamento. Os planos de engajamento serão abordados mais adiante nesta sala.

A próxima etapa fundamental para um engajamento preciso e transparente é um escopo bem definido. O escopo de um engajamento variará de acordo com a organização e com a aparência de sua infraestrutura e postura. O escopo de um cliente normalmente definirá o que você não pode fazer ou almejar; também pode incluir o que você pode fazer ou almejar.

Embora os objetivos do cliente possam ser discutidos e determinados junto com a equipe fornecedora, um escopo deve ser definido apenas pelo cliente. Eles devem ter um entendimento claro de sua rede e das implicações de uma avaliação. As especificidades do escopo e da redação sempre parecerão diferentes, abaixo está um exemplo de como a verborragia pode parecer dentro do escopo de um cliente.

Ao analisar os objetivos ou escopos de um cliente a partir de uma perspectiva de equipe vermelha, é essencial entender o significado e as implicações mais profundos. Ao analisar, você deve sempre ter um entendimento dinâmico de como sua equipe abordaria os problemas/objetivos. Se necessário, você deve escrever seus planos de engajamento ou iniciá-los apenas com uma leitura simples dos objetivos e escopo do cliente.

2.Regras de engajamento (RoE)

RoE são um esboço juridicamente vinculativo dos objetivos e escopo do cliente com mais detalhes das expectativas de engajamento entre ambas as partes. Este é o primeiro documento "oficial" no processo de planejamento de engajamento e requer autorização adequada entre o cliente e a equipe vermelha.

Este documento geralmente atua como um contrato geral entre as duas partes; um contrato externo ou outros NDAs (Acordo de Não Divulgação) também podem ser usados. O formato e a redação do RoE são essenciais, pois é um contrato juridicamente vinculativo e define expectativas claras. Abaixo está uma breve tabela de seções padrão que você pode ver contidas no RoE.

Seção	Detalhes
Sumário executivo	Resumo abrangente de todos os conteúdos e autorizações dentro do documento RoE
Propósito	Define por que o documento RoE é usado
Referências	Todas as referências usadas no documento RoE (HIPAA, ISO, etc.)
Escopo	Declaração de concordância com restrições e diretrizes
Definições	Definições de termos técnicos usados em todo o documento RoE
Regras de engajamento	Define as obrigações de ambas as partes e as expectativas técnicas gerais da conduta do trabalho
Provisionamento	Defina exceções e informações adicionais das Regras de Engajamento
Requerimentos, restrições e autoridades	Definir expectativas específicas da célula da equipe vermelha
Regras base	Definir limitações das interações da célula da equipe vermelha
Resolução de problemas	Contém todo o pessoal essencial envolvido em um engajamento
Autorização	Declaração de autorização para o engajamento
Aprovação	Assinaturas de ambas as partes aprovando todas as subseções do documento anterior
Apêndice	Qualquer informação adicional das subseções anteriores

3.Planejamento de campanha

O planejamento de campanha usa as informações adquiridas e planejadas dos objetivos do cliente e do RoE e as aplica a vários planos e documentos para identificar como e o que o *red team* fará.

Cada equipe vermelha interna terá sua metodologia e documentação para planejamento de campanha. Mostraremos um conjunto aprofundado de planos que permite comunicação precisa e documentação detalhada. O resumo da campanha que usaremos consiste em quatro planos diferentes variando em profundidade e cobertura

adaptados de documentos de operações militares. Cada plano pode ser encontrado na tabela abaixo com uma breve explicação.

Tipo de plano	Explicação	Conteúdo do plano
Engajamento	Uma descrição abrangente dos requisitos técnicos do *red team*	CONOPS, Requisitos de Recursos e Pessoal, Cronogramas
Operações	Uma expansão do plano de engajamento. Vai mais a fundo nas especificidades de cada detalhe	Operadores, Informações Conhecidas, Responsabilidades, etc
Missão	Os comandos exatos para executar e o tempo de execução do engajamento	Comandos para executar, Objetivos de tempo, Operador responsável, etc
Remediação	Define como o engajamento prosseguirá após o término da campanha	Relatório, consulta de remediação, etc

A documentação de engajamento é uma extensão do planejamento de campanha onde ideias e pensamentos do planejamento de campanha são oficialmente documentados.

3.1 Planos de engajamento

3.1.1 CONOPS (Concept of Operations)

Visão geral escrita de forma não técnica sobre como a equipe vermelha atende aos objetivos do cliente e direciona o cliente

3.1.2 Requisitos de recursos

Inclui cronogramas e informações necessárias para que a equipe vermelha tenha sucesso. Quaisquer requisitos de recursos: pessoal, hardware, requisitos de nuvem

3.2 Planos de operação

3.2.1 *Personnel*

Informações sobre os requisitos dos funcionários

3.2.2 Condições de parada

Como e por que a equipe vermelha deve parar durante o combate

3.2.3 Requisitos técnicos e ROE

Que conhecimento o *red team* precisará para ter sucesso

3.3 Planos de missão

3.3.1 Comandos para execução (opcional)

Comandos e ferramentas exatas para executar, incluindo quando, por que e como. Comumente visto em equipes maiores com muitos operadores em vários níveis de habilidade

3.3.2 Número de execuções

Horários para começar estágios de engajamento. Opcionalmente, pode incluir horários exatos para executar ferramentas e comandos

3.3.3 Responsabilidades/papéis

Quem faz o quê, quando

3.4 Planos de remediação

3.4.1 Relatório

Resumo dos detalhes do envolvimento e relatório das conclusões

3.4.2 Remediação/consulta

Como o cliente irá remediar as descobertas? Pode ser incluído no relatório ou discutido em uma reunião entre o cliente e o *red team*

4.Conceito das operações

O Conceito de Operação (CONOPS) é uma parte do plano de engajamento que detalha uma visão geral de alto nível dos procedimentos de um engajamento; podemos comparar isso a um resumo executivo de um relatório de teste de penetração. O documento servirá como uma referência de negócios/cliente e uma referência para a célula vermelha construir e estender para planos de campanha futuros.

O documento CONOPS deve ser escrito a partir de uma perspectiva de resumo semi técnico, assumindo que o público-alvo/leitor tem zero ou conhecimento técnico mínimo. Embora o CONOPS deva ser escrito em alto nível, você não deve omitir detalhes como ferramentas comuns, grupo-alvo, etc. Como na maioria dos documentos da equipe vermelha, não há um padrão definido de um documento CONOPS. Abaixo está um esboço de componentes críticos que devem ser incluídos em um CONOPS:

- Nome do cliente
- Serviço providenciado
- Tempo
- Objetivos gerais
- Outros objetivos
- Ferramentas/técnicas
- Ameaças de grupos para simulação

5.Planos de recursos

O plano de recursos é o segundo documento do plano de engajamento, detalhando uma breve visão geral de datas, conhecimento necessário (opcional), requisitos de recursos. O plano estende o CONOPS e inclui detalhes específicos, como datas, conhecimento necessário, etc. Ao contrário do CONOPS, o plano de recursos não deve ser escrito como um resumo; em vez disso, escrito como listas com marcadores de subseções. Como na maioria dos documentos da equipe vermelha, não há um conjunto padrão de modelos ou documentos de plano de recursos. Abaixo, uma lista de exemplos de subseções de planos de recursos:

- **Header:** Datas, clientes
- **Datas de engajamento:** Datas para *reconhecimento*, datas de compromisso, pós-exploração e persistência, etc
- **Conhecimento necessário:** Reconhecimento, comprometimento inicial, pós-exploração
- **Recursos necessários:** Hardware, Cloud, etc

6.Planos de operação

O plano de operações é um documento(s) flexível(is) que fornece detalhes específicos do engajamento e das ações que ocorrem. O plano expande o CONOPS atual e deve incluir a maioria das informações específicas do engajamento. O ROE também pode ser colocado aqui dependendo da profundidade e estrutura do ROE.

O plano de operações deve seguir um esquema de escrita similar ao plano de recursos, usando listas com marcadores e pequenas subseções. Assim como nos outros documentos da equipe vermelha, não há um conjunto padrão de modelos ou documentos de plano de operação. Abaixo está um esboço de subseções de exemplo dentro do plano de operações:

- **Header:** Datas e clientes
- Condições de começo/parada
- Assinatura pessoal
- TTPs específicas e ataques planejados
- Planos de comunicação
- RoE (Opcional)

7.Planos de missão

O plano de missão é um documento específico da célula que detalha as ações exatas a serem concluídas pelos operadores. O documento usa informações de planos anteriores e atribui ações a eles. Como o documento é escrito e detalhado

dependerá da equipe; como este é um documento usado internamente, a estrutura e os detalhes têm menos impacto. Como em todos os documentos descritos nesta sala, a apresentação pode variar; este plano pode ser tão simples quanto enviar um e-mail para todos os operadores. Abaixo está uma lista dos detalhes mínimos que as células devem incluir no plano:

- Objetivos
- Operadores
- Exploits/ataques
- Alvos (usuários/máquinas/objetivos)
- Planos de execução