1.Introdução

Operations Security (OPSEC) é um termo cunhado pelo exército dos Estados Unidos. No campo da segurança cibernética, vamos começar com a definição fornecida pelo NIST: "*Processo sistemático e comprovado pelo qual adversários em potencial podem ter informações negadas sobre capacidades e intenções por meio da identificação, controle e proteção de evidências geralmente não classificadas do planejamento e execução de atividades sensíveis. O processo envolve cinco etapas:* ***identificação de informações críticas, análise de ameaças, análise de vulnerabilidades, avaliação de riscos*** *e* ***aplicação de contramedidas apropriadas****"*.

Negar a qualquer adversário em potencial a capacidade de reunir informações sobre nossas capacidades e intenções é essencial para manter o OPSEC. OPSEC é um processo para identificar, controlar e proteger qualquer informação relacionada ao planejamento e execução de nossas atividades. Estruturas como o Cyber Kill Chain da Lockheed Martin e o MITRE ATT&CK ajudam os defensores a identificar os objetivos que um adversário está tentando atingir.

O MITRE ATT&CK está indiscutivelmente na vanguarda da reportagem e classificação de táticas, técnicas e procedimentos (TTPs) do adversário e oferece uma base de conhecimento acessível publicamente como inteligência de ameaças e relatórios de incidentes disponíveis publicamente como sua principal fonte de dados.

O processo OPSEC tem cinco etapas:

- Identificar informações críticas
- Analisar ameaças
- Analisar vulnerabilidades
- Avaliar riscos
- Aplicar contramedidas

OPSEC não é uma solução ou um conjunto de regras. OPSEC é um processo de cinco etapas para negar que adversários tenham acesso a qualquer informação crítica.

2.Identificação de informações críticas

Informações críticas incluem, mas não estão limitadas a, intenções, capacidades, atividades e limitações da equipe vermelha. Informações críticas incluem qualquer informação que, uma vez obtida pelo *blue team*, possa atrapalhar ou degradar a missão de *red team*.

Para identificar informações críticas, a equipe *red team* precisa usar uma abordagem adversária e se perguntar quais informações um adversário, o *blue team*, neste caso, gostaria de saber sobre a missão. Se obtidas, o adversário estará em

uma posição sólida para frustrar os ataques de *red team*. Portanto, informações críticas não são necessariamente informações sensíveis; no entanto, são quaisquer informações que podem prejudicar seus planos se vazadas para um adversário.

A seguir estão alguns exemplos:

- Informações do cliente que sua equipe aprendeu. É inaceitável compartilhar informações específicas do cliente, como nomes de funcionários, funções e infraestrutura que sua equipe descobriu. Compartilhar esse tipo de informação deve ser mantido na base da necessidade de saber, pois pode comprometer a integridade da operação. O Princípio do Menor Privilégio (PoLP) determina que qualquer entidade (usuário ou processo) deve ser capaz de acessar apenas as informações necessárias para executar sua tarefa. O PoLP deve ser aplicado em cada etapa tomada pelo *red team*.
- Informações de *red team*, como identidades, atividades, planos, capacidades e limitações. O adversário pode usar essas informações para estar melhor preparado para enfrentar seus ataques.
- Táticas, técnicas e procedimentos (TTP) que sua equipe usa para emular um ataque.
- SO, provedor de hospedagem em nuvem ou framework C2 utilizado pela sua equipe. Digamos que sua equipe use o Pentoo para testes de penetração, e o defensor sabe disso. Consequentemente, eles podem ficar de olho nos logs que expõem o SO como Pentoo. Dependendo do alvo, há uma possibilidade de que outros invasores também estejam usando o Pentoo para lançar seus ataques; no entanto, não há razão para expor seu SO se você não precisar.
- Endereços IP públicos que sua *red team* usará. Se o *blue team* obtiver acesso a esse tipo de informação, ela poderá rapidamente mitigar o ataque bloqueando todo o tráfego de entrada e saída para seus endereços IP, deixando você para descobrir o que aconteceu.
- Nomes de domínio (DNS) que sua equipe registrou. Nomes de domínio desempenham um papel significativo em ataques como phishing. Da mesma forma, se o *blue team* descobrir os nomes de domínio que você usará para lançar seus ataques, eles podem simplesmente bloquear ou fazer sinkhole em seus domínios maliciosos para neutralizar seu ataque.
- Sites hospedados, como sites de phishing, para emulação de adversários

3.Análise de ameaças

Após identificarmos informações críticas, precisamos analisar ameaças. Análise de ameaças se refere à identificação de adversários em potencial e suas intenções e capacidades. Adaptado do Manual do Programa de Segurança de Operações (OPSEC)

do Departamento de Defesa dos EUA (DoD), a análise de ameaças visa responder às seguintes perguntas:

- Quem é o adversário?
- Qual o objetivo do adversário?
- Quais táticas, técnicas e procedimentos o adversário utiliza?
- Qual informação crítica o adversário obteve?

A tarefa de *red team* é emular um ataque real para que o *blue team* descubra suas deficiências, se houver, e se torne mais bem preparada para enfrentar as ameaças que chegam. O principal objetivo de *blue team* é garantir a segurança da rede e dos sistemas da organização. As intenções são claras; eles querem manter o *red team* fora de sua rede. Consequentemente, considerando a tarefa do *red team*, a tarefa do *blue team* é considerada nossa adversária, pois cada equipe tem objetivos conflitantes. Devemos observar que as capacidades do *blue team* podem nem sempre ser conhecidas no início.

Jogadores maliciosos de terceiros podem ter diferentes intenções e capacidades e podem pausar uma ameaça como resultado. Essa parte pode ser alguém com capacidades humildes escaneando os sistemas aleatoriamente em busca de frutos fáceis, como um servidor explorável sem patch, ou pode ser um adversário capaz mirando sua empresa ou seus sistemas de cliente. Consequentemente, as intenções e as capacidades dessa terceira parte podem torná-la um adversário também.

Consideramos qualquer adversário com a intenção e capacidade de tomar ações que nos impeçam de concluir nossa operação como uma ameaça: **ameaça = adversário + intenções + capacidade**

4.Análise de vulnerabilidades

Após identificar informações críticas e analisar ameaças, podemos começar com o terceiro passo: analisar vulnerabilidades. Isso não deve ser confundido com vulnerabilidades relacionadas à segurança cibernética. Uma vulnerabilidade OPSEC existe quando um adversário pode obter informações críticas, analisar as descobertas e agir de uma forma que afetaria seus planos.

Para entender melhor uma vulnerabilidade OPSEC relacionada ao red teaming, consideraremos o seguinte cenário. Você usa o Nmap para descobrir hosts ativos em uma sub-rede alvo e encontrar portas abertas em hosts ativos. Além disso, você envia vários e-mails de phishing que levam a vítima a uma página da web de phishing que você está hospedando. Além disso, você está usando a estrutura Metasploit para tentar explorar certas vulnerabilidades de software. Essas são três atividades separadas; no entanto, se você usar o(s) mesmo(s) endereço(s) IP para realizar essas atividades diferentes, isso levaria a uma vulnerabilidade OPSEC.

Uma vez que qualquer atividade hostil/maliciosa é detectada, espera-se que a equipe azul tome medidas, como bloquear o(s) endereço(s) IP de origem temporariamente ou permanentemente. Consequentemente, seria necessário que um endereço IP de origem fosse bloqueado para que todas as outras atividades que usam esse endereço IP falhassem. Em outras palavras, isso bloquearia o acesso ao endereço IP de destino usado para o servidor de phishing e ao endereço IP de origem usado pelo Nmap e Metasploit Framework.

Outro exemplo de uma vulnerabilidade OPSEC seria um banco de dados não seguro que é usado para armazenar dados recebidos de vítimas de phishing. Se o banco de dados não estiver devidamente protegido, isso pode levar a um terceiro malicioso a comprometer a operação e pode resultar em dados sendo exfiltrados e usados em um ataque contra a rede do seu cliente. Como resultado, em vez de ajudar seu cliente a proteger sua rede, você acabaria ajudando a expor nomes de login e senhas.

OPSEC fraco também pode resultar em vulnerabilidades menos sofisticadas. Por exemplo, considere um caso em que um dos membros da sua equipe vermelha publica em mídias sociais revelando o nome do seu cliente. Se a equipe azul monitorar essas informações, isso os levará a aprender mais sobre sua equipe e suas abordagens para se preparar melhor contra tentativas de penetração esperadas.

5.Avaliações de risco

O NIST define uma avaliação de risco como "*O processo de identificação de riscos para operações organizacionais (incluindo missão, funções, imagem, reputação), ativos organizacionais, indivíduos, outras organizações e a Nação, resultantes da operação de um sistema de informação*". Em OPSEC, a avaliação de risco requer o aprendizado da possibilidade de um evento ocorrer junto com o custo esperado desse evento. Consequentemente, isso envolve avaliar a capacidade do adversário de explorar as vulnerabilidades.

Uma vez que o nível de risco é determinado, contramedidas podem ser consideradas para mitigar esse risco. Precisamos considerar os três fatores a seguir:

- A eficiência da contramedida na redução do risco
- O custo da contramedida comparado ao impacto da vulnerabilidade que está sendo explorada
- A possibilidade de que a contramedida possa revelar informações ao adversário

Vamos revisitar os dois exemplos da tarefa anterior. No primeiro exemplo, consideramos a vulnerabilidade de escanear a rede com Nmap, usando a estrutura Metasploit e hospedando as páginas de phishing usando o mesmo endereço IP público. Analisamos que isso é uma vulnerabilidade, pois torna mais fácil para o adversário bloquear nossas três atividades simplesmente detectando uma atividade. Agora, vamos

avaliar esse risco. Para avaliar o risco relacionado a essa vulnerabilidade, precisamos aprender a possibilidade de uma ou mais dessas atividades serem detectadas.

Não podemos responder a isso sem obter algumas informações sobre os recursos do adversário. Vamos considerar o caso em que o cliente tem um Security Information and Event Management (SIEM) em vigor. Um SIEM é um sistema que permite o monitoramento e a análise em tempo real de eventos relacionados à segurança de diferentes fontes na rede. Podemos esperar que um SIEM tornaria razoavelmente descomplicado detectar atividades suspeitas e conectar os três eventos. Como resultado, avaliaríamos o risco relacionado como alto. Por outro lado, se sabemos que o adversário tem recursos mínimos para detectar eventos de segurança, podemos avaliar o risco relacionado a essa vulnerabilidade como baixo.

6.Contramedidas

A etapa final é aplicar contramedidas. O Manual do Programa de Segurança de Operações (OPSEC) do Departamento de Defesa dos EUA (DoD) afirma: "*Contramedidas são projetadas para impedir que um adversário detecte informações críticas, forneça uma interpretação alternativa de informações ou indicadores críticos (engano) ou negue o sistema de coleta do adversário*".

Vamos revisitar os dois exemplos que apresentamos na tarefa de Análise de Vulnerabilidade. No primeiro exemplo, consideramos a vulnerabilidade de executar o Nmap, usando a estrutura Metasploit e hospedando as páginas de phishing usando o mesmo endereço IP público. A contramedida para isso parece óbvia; use um endereço IP diferente para cada atividade. Dessa forma, você pode garantir que, se uma atividade for detectada, o endereço IP público será bloqueado, as outras atividades podem continuar sem serem afetadas.

No segundo exemplo, consideramos a vulnerabilidade de um banco de dados não seguro usado para armazenar dados recebidos de uma página de phishing. De uma perspectiva de avaliação de risco, consideramos isso como alto risco devido a terceiros maliciosos potencialmente procurando alvos fáceis aleatórios. A contramedida, neste caso, seria garantir que o banco de dados esteja adequadamente protegido para que os dados não possam ser acessados, exceto por pessoal autorizado.