1.Introdução

O reconhecimento ativo exige que você faça algum tipo de contato com seu alvo. Esse contato pode ser um telefonema ou uma visita à empresa alvo sob algum pretexto para coletar mais informações, geralmente como parte da engenharia social. Alternativamente, pode ser uma conexão direta com o sistema alvo, seja visitando seu site ou verificando se seu firewall tem uma porta SSH aberta. Pense nisso como se você estivesse inspecionando janelas e fechaduras de portas de perto. Portanto, é essencial lembrar de não se envolver em trabalho de reconhecimento ativo antes de obter autorização legal assinada pelo cliente.

O reconhecimento ativo começa com conexões diretas feitas à máquina alvo. Qualquer conexão desse tipo pode deixar informações nos logs mostrando o endereço IP do cliente, hora da conexão e duração da conexão, entre outras coisas.

No entanto, nem todas as conexões são suspeitas. É possível deixar seu reconhecimento ativo aparecer como atividade regular do cliente. Considerando a navegação na web, ninguém suspeitaria de um navegador conectado a um servidor web alvo entre centenas de outros usuários legítimos. Você pode usar essas técnicas a seu favor ao trabalhar como parte de *red team* e não quer alarmar o *blue team*.

2.Navegadores web

O navegador da web pode ser uma ferramenta conveniente, especialmente porque está prontamente disponível em todos os sistemas. Há várias maneiras de usar um navegador da web para coletar informações sobre um alvo, como:

- porta TCP 80 por padrão quando um site é acessado via HTTP
- porta TCP 443 por padrão quando um site é acessado via HTTPS

O navegador web O navegador da web não os mostra na barra de endereços. No entanto, é possível usar portas personalizadas para acessar um serviço, por exemplo, o endereço **https://127.0.0.1:8834** irá conectar em 127.0.0.1 (localhost) na porta 8834 via protocolo HTTPS. Se existir um servidor escutando naquela porta, receberemos uma página web.

Em um computador, enquanto você navega, você pode pressionar **ctrl+shift+I** para abrir as ferramentas de desenvolvedor (Firefox). **As ferramentas de desenvolvedor permitem que você inspecione muitas coisas que seu navegador recebeu e trocou com o servidor remoto**. Por exemplo, você pode visualizar e até mesmo modificar os arquivos JavaScript (JS), inspecionar os cookies definidos no seu sistema e descobrir a estrutura de pastas do conteúdo do site.

Também há muitos complementos para Firefox e Chrome que podem ajudar em testes de penetração. Aqui estão alguns exemplos:

- **FoxyProxy** permite que você altere rapidamente o servidor proxy que está usando para acessar o site de destino. Esta extensão do navegador é conveniente quando você está usando uma ferramenta como o Burp Suite ou se você precisa alternar servidores proxy regularmente
- **User-Agent Switcher and Manager** dá a você a habilidade de fingir que está acessando a página da web de um sistema operacional diferente ou navegador da web diferente. Em outras palavras, você pode fingir que está navegando em um site usando um iPhone quando, na verdade, está acessando-o do Mozilla Firefox.
- **Wappalyzer** fornece *insights* sobre as tecnologias usadas nos sites visitados. Essa extensão é útil, principalmente quando você coleta todas essas informações enquanto navega no site como qualquer outro usuário.

3.O comando Ping

O propósito principal do ping é verificar se você consegue alcançar o sistema remoto e se o sistema remoto consegue alcançar você de volta. Em outras palavras, inicialmente, isso era usado para verificar a conectividade de rede; no entanto, estamos mais interessados em seus diferentes usos: verificar se o sistema remoto está online.

Em termos simples, o comando ping envia um pacote para um sistema remoto, e o sistema remoto responde. Dessa forma, você pode concluir que o sistema remoto está online e que a rede está funcionando entre os dois sistemas.

Se você preferir uma definição mais exigente, o ping é um comando que envia um pacote ICMP Echo para um sistema remoto. Se o sistema remoto estiver online, e o pacote ping foi roteado corretamente e não bloqueado por nenhum firewall, o sistema remoto deve enviar de volta uma ICMP Echo Reply. Da mesma forma, a resposta ping deve chegar ao primeiro sistema se for roteado apropriadamente e não for bloqueada por nenhum firewall.

Quando não recebemos uma resposta de ping, há algumas explicações que podem explicar por que não recebemos uma resposta de ping, por exemplo:

- O computador de destino não está respondendo
- Está desconectado da rede ou algum problema impede a comunicação
- Um firewall está configurado para bloquear este tipo de pacote
- O seu sistema está fora da rede

4.Traceroute

Como o nome sugere, o comando traceroute rastreia a rota tomada pelos pacotes do seu sistema para outro host. O propósito de um traceroute é encontrar os endereços

IP dos roteadores ou hops que um pacote atravessa conforme ele vai do seu sistema para um host de destino.

Este comando também revela o número de roteadores entre os dois sistemas. Ele é útil, pois indica o número de hops (roteadores) entre seu sistema e o host de destino. No entanto, observe que a rota tomada pelos pacotes pode mudar, pois muitos roteadores usam protocolos de roteamento dinâmico que se adaptam a mudanças de rede.

Não há uma maneira direta de descobrir o caminho do seu sistema para um sistema de destino. Contamos com o ICMP para "enganar" os roteadores para que revelem seus endereços IP. Podemos fazer isso usando um pequeno Time To Live (TTL) no campo de cabeçalho IP. Embora o T em TTL signifique tempo, TTL indica o número máximo de roteadores/saltos pelos quais um pacote pode passar antes de ser descartado; TTL não é um número máximo de unidades de tempo. Quando um roteador recebe um pacote, ele diminui o TTL em um antes de passá-lo para o próximo roteador.

No entanto, se o TTL atingir 0, ele será descartado, e um ICMP Time-to-Live excedido será enviado ao remetente original. Na figura a seguir, o sistema definiu o TTL como 1 antes de enviá-lo ao roteador. O primeiro roteador no caminho diminui o TTL em 1, resultando em um TTL de 0. Consequentemente, esse roteador descartará o pacote e enviará uma mensagem de erro em trânsito ICMP time exceeded. Observe que alguns roteadores são configurados para não enviar essas mensagens ICMP ao descartar um pacote.

Para resumir, podemos implicar o seguinte:

- O número de hops/roteadores entre seu sistema e o sistema de destino depende do tempo em que você está executando o traceroute. Não há garantia de que seus pacotes sempre seguirão a mesma rota, mesmo se você estiver na mesma rede ou se repetir o comando traceroute em um curto espaço de tempo
- Alguns roteadores retornam um endereço IP público. Você pode examinar alguns desses roteadores com base no escopo do teste de penetração pretendido
- Alguns roteadores não retornam uma resposta

5.Telnet

Este protocolo foi desenvolvido em 1969 para se comunicar com um sistema remoto por meio de uma interface de linha de comando (CLI). A porta padrão usada pelo telnet é 23. De uma perspectiva de segurança, o telnet envia todos os dados, incluindo nomes de usuários e senhas, em texto simples. Enviar em texto simples torna fácil para qualquer um, que tenha acesso ao canal de comunicação, roubar as credenciais de login. A alternativa segura é o protocolo SSH.

No entanto, o cliente telnet, com sua simplicidade, pode ser usado para outros propósitos. Sabendo que o cliente telnet depende do protocolo TCP, você pode usar o Telnet para se conectar a qualquer serviço e pegar seu banner.

6.Netcat

O Netcat suporta os protocolos TCP e UDP. Ele pode funcionar como um cliente que se conecta a uma porta de escuta; alternativamente, ele pode atuar como um servidor que escuta em uma porta de sua escolha. Portanto, é uma ferramenta conveniente que você pode usar como um cliente ou servidor simples sobre TCP ou UDP. Você pode usar o netcat para escutar em uma porta TCP e se conectar a uma porta de escuta em outro sistema.