1.Introdução

Antes do surgimento dos sistemas e redes de computadores, na Arte da Guerra, Sun Tzu ensinou: "Se você conhece o inimigo e conhece a si mesmo, sua vitória não ficará em dúvida". Se você está desempenhando o papel de um atacante, precisa reunir informações sobre seus sistemas-alvo. Se você está desempenhando o papel de um defensor, precisa saber o que seu adversário descobrirá sobre seus sistemas e redes.

Reconhecimento (recon) pode ser definido como uma pesquisa preliminar para reunir informações sobre um alvo. É o primeiro passo na The Unified Kill Chain para ganhar uma posição inicial em um sistema. Dividimos o reconhecimento em:

- Reconhecimento passivo
- Reconhecimento ativo

No reconhecimento passivo, você confia no conhecimento disponível publicamente. É o conhecimento que você pode acessar de recursos disponíveis publicamente sem se envolver diretamente com o alvo. Pense nisso como se estivesse olhando para o território alvo de longe sem pisar naquele território.

As atividades de reconhecimento passivo incluem muitas atividades, por exemplo:

- Buscar por registros de DNS de um domínio de um servidor DNS público
- Verificar por buscas de trabalhos relacionados ao website
- Ler artigos sobre a empresa alvo

2.whois

WHOIS é um protocolo de solicitação e resposta que segue a especificação RFC 3912. Um servidor WHOIS escuta na porta TCP 43 para solicitações de entrada. O registrador de domínio é responsável por manter os registros WHOIS para os nomes de domínio que está alugando. O servidor WHOIS responde com várias informações relacionadas ao domínio solicitado.

De particular interesse, podemos aprender:

- **Registrar:** Por meio de qual registrador o nome de domínio foi registrado?
- **Informações de contato:** Nome, organização, endereço, telefone, entre outras coisas. (a menos que sejam ocultados por meio de um serviço de privacidade)
- **Criação, data de expiração e atualização:** Quando o nome de domínio foi registrado pela primeira vez? Quando foi atualizado pela última vez? E quando precisa ser renovado?
- **Nomes de servidores:** Qual servidor pedir para resolver o nome de domínio?

Muitos serviços online fornecem informações whois; no entanto, geralmente é mais rápido e conveniente usar seu cliente whois local.

3.DNSDumpster

Ferramentas de pesquisa de DNS, como nslookup e dig, não conseguem encontrar subdomínios por si só. O domínio que você está inspecionando pode incluir um subdomínio diferente que pode revelar muitas informações sobre o alvo. Por exemplo, se tryhackme.com tem os subdomínios wiki.tryhackme.com e webmail.tryhackme.com, você quer aprender mais sobre esses dois, pois eles podem conter um tesouro de informações sobre seu alvo. Há uma possibilidade de que um desses subdomínios tenha sido configurado e não seja atualizado regularmente. A falta de atualizações regulares adequadas geralmente leva a serviços vulneráveis.

Podemos considerar usar vários mecanismos de busca para compilar uma lista de subdomínios conhecidos publicamente. Um mecanismo de busca não será suficiente; além disso, devemos esperar passar por pelo menos dezenas de resultados para encontrar dados interessantes. Afinal, você está procurando por subdomínios que não são anunciados explicitamente e, portanto, não é necessário chegar à primeira página de resultados de busca. Outra abordagem para descobrir esses subdomínios seria confiar em consultas de força bruta para encontrar quais subdomínios têm registros DNS.

Para evitar uma busca tão demorada, pode-se usar um serviço online que oferece respostas detalhadas às consultas de DNS, como o DNSDumpster. O DNSDumpster também representará as informações coletadas graficamente.

4.Shodan.io

Quando você é encarregado de executar um teste de penetração contra alvos específicos, como parte da fase de reconhecimento passivo, um serviço como o Shodan.io pode ser útil para aprender várias informações sobre a rede do cliente, sem se conectar ativamente a ela. Além disso, no lado defensivo, você pode usar diferentes serviços do Shodan.io para aprender sobre dispositivos conectados e expostos pertencentes à sua organização.

Shodan.io tenta se conectar a todos os dispositivos acessíveis online para construir um mecanismo de busca de “coisas” conectadas em contraste com um mecanismo de busca para páginas da web. Uma vez que obtém uma resposta, ele coleta todas as informações relacionadas ao serviço e as salva no banco de dados para torná-las pesquisáveis. Considere o registro salvo de um dos servidores do tryhackme.com.

Este registro mostra um servidor web; no entanto, como já mencionado, o Shodan.io coleta informações relacionadas a qualquer dispositivo que possa encontrar

conectado online. Por meio deste resultado de pesquisa no Shodan.io, podemos aprender várias coisas relacionadas à nossa pesquisa, como:

- Endereços IP
- Empresa host
- Localização geográfica
- Tipos e versões do servidor

Você também pode tentar procurar os endereços IP que você obteve de pesquisas de DNS. Esses são, é claro, mais sujeitos a mudanças.