1.Análise de rede: Tráfego TCP/IP

1.1 Avaliação da segurança organizacional

A avaliação de segurança refere-se a processos e ferramentas que avaliam a superfície de ataque. Com o conhecimento das táticas e capacidades do adversário, você pode avaliar se os pontos na superfície de ataque são vetores de ataque potencialmente vulneráveis. O resultado da avaliação são recomendações para implantar, aprimorar ou reconfigurar controles de segurança para mitigar o risco de vulnerabilidades serem exploradas por agentes de ameaças.

2.Ferramentas de detecção de rede

O reconhecimento é um tipo de atividade de avaliação que mapeia a superfície de ataque potencial, identificando os nós e conexões que compõem a rede. Periodicamente, você precisará executar varreduras usando ferramentas de descoberta de topologia por meio de linha de comando e interface gráfica de usuário.

O processo de mapeamento da superfície de ataque é conhecido como reconhecimento e descoberta de rede. As técnicas de reconhecimento podem ser usadas por agentes de ameaças, mas também por profissionais de segurança para sondar e testar seus próprios sistemas de segurança, como parte de uma avaliação de segurança e monitoramento contínuo.

A descoberta de topologia também pode ser usada para construir um banco de dados de ativos e para identificar hosts não autorizados ou erros de configuração de rede. Tarefas básicas de descoberta de topologia podem ser realizadas usando as ferramentas de linha de comando integradas ao Windows e ao Linux. As ferramentas a seguir relatam a configuração IP e testam a conectividade no segmento ou sub-rede da rede local.

- **ipconfig:** Mostra a configuração atribuída às interfaces de rede no Windows, incluindo o endereço de hardware ou controle de acesso à mídia (MAC), endereços IPv4 e IPv6, gateway padrão e se o endereço é estático ou atribuído por DHCP. Se o endereço for atribuído por DHCP, a saída também mostrará o endereço do DHCP servidor que forneceu a concessão.
- **ifconfig:** Mostra a configuração atribuída às interfaces de rede no Linux.
- **ping:** Investiga um host em um determinado endereço IP ou nome de host usando o Internet Control Message Protocol (ICMP). Você pode usar o ping com um script simples para realizar uma varredura de todos os endereços IP em uma sub-rede
- **arp:** Exibe o cache do protocolo de resolução de endereço (ARP) da máquina local. O cache ARP mostra o endereço MAC da interface associada a cada endereço IP com o qual o host local se comunicou recentemente. Isso pode ser útil se você estiver investigando uma suspeita de ataque de falsificação.

2.1 Configurações de rotas

As ferramentas a seguir podem ser usadas para testar a configuração de roteamento e a conectividade com hosts e redes remotas:

- **route:** Visualize e configure a tabela de roteamento local do host. A maioria dos sistemas finais usa uma rota padrão para encaminhar todo o tráfego para redes remotas através de um roteador gateway. Se o host não for um roteador, entradas adicionais na tabela de roteamento poderão ser suspeitas.
- **tracert:** Usa testes ICMP para relatar o tempo de ida e volta (RTT) para saltos entre o host local e um host em uma rede remota. tracert é a versão Windows da ferramenta.
- **traceroute:** Realiza descoberta de rotas a partir de um host Linux. traceroute usa testes UDP em vez de ICMP, por padrão.
- **pathping:** Fornece estatísticas de latência e perda de pacotes ao longo de uma rota durante um período de medição mais longo. O pathping é uma ferramenta do MS-Windows; o equivalente no Linux é **mtr**. A alta latência em outros saltos pode ser um sinal de negação ou serviço, ou apenas indicar congestionamento na rede.

3.Scanners IP e Nmap

A varredura de uma rede usando ferramentas como ping consome tempo, não é confiável e não retorna resultados detalhados. A maior parte da descoberta de topologia é realizada usando uma ferramenta de scanner IP dedicada. Um scanner IP realiza a descoberta de hosts e identifica como os hosts estão conectados em uma rede.

O Nmap Security Scanner é um dos scanners IP de código aberto mais populares. O Nmap pode usar diversos métodos de descoberta de host, alguns dos quais podem operar furtivamente e servir para derrotar mecanismos de segurança, como firewalls e detecção de intrusões. A ferramenta é um software de código aberto com pacotes para a maioria das versões do Windows, Linux e macOS. Pode ser operado com linha de comando ou via GUI.

3.1 Descobertas de serviço e o Nmap

Tendo identificado hosts IP ativos na rede e obtido uma ideia da topologia da rede, o próximo passo no reconhecimento da rede é descobrir quais sistemas operacionais estão em uso, quais serviços de rede cada host está executando e, se possível, qual software aplicativo está sustentando esses serviços. Este processo é descrito como descoberta de serviço. A descoberta de serviços também pode ser usada defensivamente, para investigar possíveis sistemas não autorizados e identificar a presença de portas de serviços de rede não autorizadas.

- **TCP SYN (-sS):** Esta é uma técnica rápida também conhecida como varredura semiaberta, pois o host de varredura solicita uma conexão sem reconhecê-la. A resposta do alvo ao pacote SYN da varredura identifica o estado da porta.
- **Varreduras UDP (-sU):** Verifica portas UDP. Como estes não usam ACKs, o Nmap precisa esperar por uma resposta ou tempo limite para determinar o estado da porta, portanto a varredura UDP pode demorar muito. Uma varredura UDP pode ser combinada com uma varredura TCP.
- **Intervalo de portas (-p):** Por padrão, o Nmap verifica 1.000 portas comumente usadas, conforme listado em seu arquivo de configuração. Use o argumento -p para especificar um intervalo de portas.

4.netstat

Mostra o estado das portas TCP/UDP na máquina local. O mesmo comando é usado no Windows e no Linux, embora com sintaxe de opções diferentes. Você pode usar o netstat para verificar configurações incorretas de serviço (talvez um host esteja executando um servidor web ou FTP que um usuário instalou sem autorização).

Você também poderá identificar conexões remotas suspeitas com serviços no host local ou do host para endereços IP remotos. Se você estiver tentando identificar malware, a saída mais útil do netstat é mostrar qual processo está escutando em quais portas.

5.nslookup/dig

Consulta registros de nomes para um determinado domínio usando um DNS específico resolvedor no Windows (nslookup) ou Linux (dig). Um invasor pode testar uma rede para descobrir se o serviço DNS está configurado incorretamente. Um DNS mal configurado pode permitir uma transferência de zona, o que dará ao invasor os registros completos de cada host no domínio, revelando muito sobre a forma como a rede está configurada.

6.Análise de pacotes e wireshark

Um analisador de protocolo funciona em conjunto com um sniffer para realizar análises de tráfego. Você pode analisar uma captura ao vivo ou abrir um arquivo de captura salva (.pcap). Os analisadores de protocolo podem decodificar um quadro capturado para revelar seu conteúdo em um formato legível. Você pode optar por visualizar um resumo do quadro ou escolher uma visualização mais detalhada que forneça informações sobre a camada OSI, protocolo, função e dados.

Wireshark é um utilitário gráfico de captura e análise de pacotes de código aberto, com pacotes de instalação para a maioria dos sistemas operacionais. Tendo escolhido a interface para escutar, a saída é exibida em uma visualização de três painéis. O painel da lista de pacotes mostra um resumo de rolagem dos quadros. O painel de detalhes do pacote mostra campos expansíveis no quadro atualmente selecionado na lista de pacotes. O painel de bytes de pacote mostra os dados brutos do quadro em hexadecimal e ASCII. O Wireshark é capaz de analisar (interpretar) os cabeçalhos e payloads de centenas de protocolos de rede.