Usando o Nmap

O Nmap fornece, de uma maneira geral, a relação de computadores e serviços ativos. Existem diversas formas e parâmetros a serem informados durante uma varredura.

Para uma melhor compreensão está sendo dividido em dois tópicos as explicações: “Métodos de Varredura” e “Opções Gerais”.

Métodos de Varredura

-sP Ping scan: Algumas vezes é necessário saber se um determinado host ou rede está no ar.

Nmap pode enviar pacotes ICMP “echo request” para verificar se determinado host ou rede está ativa. Hoje em dia, existem muitos filtros que rejeitam os pacotes ICMP “echo request”, então envia um pacote TCP ACK para a porta 80 (default) e caso receba RST o alvo está ativo.

A terceira técnica envia um pacote SYN e espera um RST ou SYN-ACK.

-sR RCP scan: Este método trabalha em conjunto com várias técnicas do Nmap.

Ele considera todas as portas TCP e UDP abertas e envia comandos NULL SunRPC, para determinar se realmente são portas RPC. É como se o comando “rpcinfo -p” estivesse sendo utilizado, mesmo através de um firewall (ou protegido por TCP wrappers).

-sS TCP SYN scan: Técnica também conhecida como “half-open”, pois não abre uma conexão TCP completa. É enviado um pacote SYN, como se ele fosse uma conexão real e aguarda uma resposta. Caso um pacote SYN-ACK seja recebido, a porta está aberta, enquanto um como resposta indica que a porta está fechada. A vantagem dessa abordagem é que poucos irão detectar esse scanning de portas.

-sT TCP connect() scan: É a técnica mais básica de TCP scanning. É utilizada a chamada de sistema (system call) “connect()” que envia um sinal as portas ativas.

Caso a porta esteja aberta recebe como resposta “connect()”. É um dos scan mais rápidos, porém fácil de ser detectado.

-sU UDP scan: Este método é utilizado para determinar qual porta UDP está aberta em um host. A técnica consiste em enviar um pacote UDP de 0 byte para cada porta do host. Se for recebido uma mensagem ICMP “port unreachable” então a porta está fechada, senão a porta pode estar aberta. Para variar um pouco.

-sV Version detection: Após as portas TCP e/ou UDP serem descobertas por algum dos métodos, o nmap irá determinar qual o serviço está rodando atualmente. O arquivo nmap-service-probes é utilizado para determinar tipos de protocolos, nome da aplicação, número da versão e outros detalhes.

-sF, **-sX**, **-sN** Stealth FIN, Xmas Tree ou Null: Alguns firewalls e filtros de pacotes detectam pacotes SYN's em portas restritas, então é necessário utilizar métodos avançados para atravessar esses softwares.

FIN: Portas fechadas enviam um pacote RST como resposta a pacotes FIN, enquanto portas abertas ignoram esses pacotes. (Esse método não funciona com a plataforma Windows, uma vez que a Microsoft não seguiu RFC 973)

Xmas Tree: Portas fechadas enviam um pacote RST como resposta a pacotes FIN, enquanto portas abertas ignoram esses pacotes. Asflags FIN, URG e PUSH são utilizados no pacotes FIN que é enviado ao alvo. (Esse método não funciona com a plataforma Windows, uma vez que a Microsoft não seguiu RFC 973)

Null: Portas fechadas enviam um pacote RST como resposta a pacotes FIN, enquanto portas abertas ignoram esses pacotes. Nenhuma flag é ligada no pacote FIN. (Esse método não funciona com a plataforma Windows, uma vez que a Microsoft não seguiu RFC 973)

Opções Gerais

-D <decoy1 [,decoy2][,VOCE],...> Durante uma varredura, utiliza uma série de endereços falsificados, simulando que o scanning tenha originado desses vários hosts, sendo raticamente impossível identifiicar a verdadeira origem da varredura.

Ex.: nmap -D IP1,IP2,IP3,IP4,IP6,SEU_IP alvo

-F Procura pelas portas que estão no /etc/services. Método mais rápido, não procura por todas as portas.

Ex.: nmap -F alvo

-I Se o host estiver utilizando o ident, é possível identificar o dono dos serviços que estão sendo executados no servidor (trabalha com a opção -sT)

Ex.: nmap -sT -I alvo

-n Não irá resolver nome de hosts a ser varrido.

Ex.: nmap -n alvo

-O Ativa a identificação do host remoto via TCP/IP. Irá apresentar versão do Sistema Operacional e tempo ativo.

Ex.: nmap -O alvo

-p <lista_de_portas> Especifica quais portas devem ser verificadas na varredura. Por default, todas as portas entre 1 e 1024 são varridas.

Ex.: nmap -p 22,80 alvo

nmap -p U:53,111,137,T:21-25,80,139,8080

-P0 Não tenta pingar o host antes de iniciar a varredura. Isto permite varrer alvos que bloqueiam ICMP “echo request (ou responses)” através de firewall.

Ex.: nmap -P0 alvo

-PS[lista_de_portas] Usa pacotes SYN para determinar se o host está ativo.

Ex.: nmap -PS80 alvo

-PT[lista_de_portas] Usa TCP “ping” para determinar se o host está ativo.

Ex.: nmap -PT80 alvo

-R Irá resolver nome de hosts a ser varrido.

Ex.: nmap -R alvo

-r A varredura será feita nas portas randomicamente, não seguinte a ordem crescente.

Ex.: nmap -r alvo

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> Esse parâmetro seta a prioridade de varredura do Nmap:

• Paranoid (-T5) é muito lento na esperança de prevenir a detecção pelo sistema IDS. Este serializa todos os scans (scanning não paralelo) e geralmente espera no mínimo 5 minutos entre o envio de pacotes.

• Sneaky (-T4) é similar ao Paranoid, exceto que somente espera 15 segundos entre o envio de pacotes.

• Polite (-T3) tem o significado para facilitar a carga na rede e reduzir as chances de travar a máquina. Ele serializa os testes e espera no mínimo 0.4 segundos entre eles.

• Normal (-T2) é o comportamento default do Nmap, o qual tenta executar tão rápido quanto possível sem sobrecarregar a rede ou perder hosts/portas.

• Aggressive(-T1) esse modo adiciona um timeout de 5 minutos por host e nunca espera mais que 1.25 segundos para testar as respostas.

• Insane (-T0) é somente adequando para redes muito rápidas ou onde você não se importa em perder algumas informações. Nesta opção o timeout dos hosts acontecem em 75 segundos e espera somente 0.3 segundos por teste individual.

-ttl <valor>

Altera o valor do TTL (Time to Live), dessa forma dificulta a origem do pacote.

Ex.: nmap -ttl 55 alvo

-v Modo verbose. Mostra tudo o que está se passando.

Ex.: nmap -v alvo

Flag não documentada

O nmap tem uma flag não documentada, a flag é: --scanflags. Com ela é possível especificar flags arbitrárias usando nomes de flags ou número. Nesse exemplo estamos usando uma varredura SYN-FIN

nmap -sS –scanflags SYNFIN -O alvo

Exemplos de utilização

Ex.: nmap -v alvo

Esta opção faz a varredura de todas as portas TCP reservadas.

Ex.: nmap -sS -O alvo/24

Lança uma varredura TCP Syn contra cada máquina que está ativa, abrangendo todas as 255 máquinas de classe “C” onde alvo faz parte. Além disso determina o sistema operacional de cada host.

Ex.: nmap -sX -p 22,53,110,143 alvo

Envia uma varredura Xmas Tree para o alvo, além de varrer somente os serviços de sshd, Dns, pop3d e imapd.