1.A ferramenta

O Nmap é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenvolvida para escanear rapidamente redes amplas, mas funciona muito bem contra hosts individuais.

Utiliza pacotes IP em estado bruto para determinar quais hosts estão disponíveis na rede, quais serviços os hosts oferecem, quais sistemas operacionais e suas versões estão em execução, que tipos de filtros de pacotes/firewall estão em uso, dentre outras.

A saída no Nmap é uma lista de alvos escaneados, com informações adicionais de cada um, dependendo das opções utilizadas. Além destas tabelas, o Nmap pode fornecer informações adicionais sobre os alvos, incluindo nomes de DNS reverso, possível sistema operacional, tipos de dispositivos e endereços MAC.

1.1 aberto (open)

Uma aplicação que está ativamente aceitando conexões TCP ou pacotes UDP nesta porta

1.2 fechado (closed)

Esta porta está acessível, mas não há nenhuma aplicação ouvindo nela. Ela recebe e responde a pacotes de sondagem do Nmap. Elas podem ser úteis para mostrar que um host está ativo em um determinado endereço IP, e como parte de uma detecção de SO.

1.3 filtrado (filtered)

O Nmap não consegue determinar se a porta está aberta porque uma filtragem de pacotes impede que as sondagens alcancem a porta. A filtragem poderia ser um dispositivo firewall dedicado, regras de roteador, ou um software de firewall baseado em host. Estas portas frustram os atacantes, pois elas fornecem poucas informações. Às vezes, elas respondem com mensagens de erro ICMP tais como as do tipo 3 código 13 (destino inalcançável: comunicação proíbida administrativamente).

1.4 não-filtrado (unfiltered)

O estado não-filtrado significa que uma porta está acessível, mas que o Nmap é incapaz de determinar se ela está aberta ou fechada. Apenas o scan ACK, que é usado para mapear conjuntos de regras de firewall, classifica portas com este estado. Escanear portas não-filtradas com outros tipos de scan, podem ajudar a responder se a porta está aberta

1.5 open | filtered

O Nmap coloca portas neste estado quando é incapaz de determinar se uma porta está aberta ou filtrada. Isso acontece para tipos de scan onde as portas abertas

não dão nenhuma resposta. A falta de resposta também pode significar que um filtro de pacotes descartou a sondagem ou qualquer resposta que ela tenha provocado. Portanto, não se sabe com certeza se a porta está aberta ou se está sendo filtrada.

1.6 closed | filtered

Este estado é usado quando o Nmap é incapaz de determinar se uma porta está fechada ou filtrada. É apenas usado para o scan IPID Idle scan

---

2.Descoberta de hosts

Um dos primeiros passos em qualquer reconhecimento de uma rede é reduzir um conjunto de faixas de endereços IP, em uma lista de hosts ativos e interessantes. **Escanear cada porta de cada endereço IP é vagaroso e normalmente desnecessário**. A descoberta de hosts às vezes é chamada de ping scan, mas vai além dos simples ***pacotes ICMP de echo request*** associados com a ferramenta.

Se nenhuma opção de descoberta de hosts for dada, o Nmap envia um pacote TCP ACK destinado a porta 80 e uma procura ***ICMP echo request*** a cada máquina-alvo. Para usuários Unix sem privilégios, com shell, um pacote SYN é enviado ao invés do ACK utilizando a chamada de sistema connect().

Por definição, o Nmap faz a descoberta de host e então executa um escaneamento de portas contra cada host que ele determina que está ativo.

2.1 Descoberta de hosts

Um dos primeiros passos em qualquer reconhecimento de uma rede é reduzir um conjunto de faixas de endereços IP, em uma lista de hosts ativos e interessantes. **Escanear cada porta de cada endereço IP é vagaroso e normalmente desnecessário**. A descoberta de hosts às vezes é chamada de ping scan, mas vai além dos simples ***pacotes ICMP de echo request*** associados com a ferramenta.

Se nenhuma opção de descoberta de hosts for dada, o Nmap envia um pacote TCP ACK destinado a porta 80 e uma procura ***ICMP echo request*** a cada máquina-alvo. Para usuários Unix sem privilégios, com shell, um pacote SYN é enviado ao invés do ACK utilizando a chamada de sistema connect().

Por definição, o Nmap faz a descoberta de host e então executa um escaneamento de portas contra cada host que ele determina que está ativo.

2.2 Scan de listagem → -sL

O scan de listagem é uma forma degenerada de descoberta de hosts que simplesmente lista cada host da rede especificada, sem enviar nenhum pacote aos hosts-alvos. Por padrão, o Nmap fará a resolução de DNS reverso dos hosts para descobrir seus nomes.

2.3 Scan usando ping → -sP

Esta opção diz ao Nmap executar somente um scan usando ping e então, mostrar os hosts disponíveis que responderam ao scan. É mais intrusivo do que o scan de listagem e pode ser usado para os mesmos propósitos. Ela envia um ***ICMP echo request*** e um pacote TCP para a porta 80 por padrão.

2.4 Scan sem ping → -P0

Esta opção pula completamente o estágio de descoberta do Nmap. Normalmente, a ferramenta utiliza este estágio para determinar as máquinas ativas para escaneamento mais agressivo.

2.5 Ping usando TCP SYN → -PS [ports]

Esta opção envia um pacote TCP vazio com a flag SYN marcada. Até uma lista de portas separadas por vírgula podem ser especificadas, por exemplo **-PS22, 23, 25, 80**. A flag SYN sugere aos sistemas remotos que você está tentando estabelecer uma comunicação. Normalmente, a porta de destino estará fechada e um pacote RST (reset) será enviado de volta. Se acontecer da porta estar aberta, o alvo irá dar o segundo passo, o ***three-way handshake*** (SYN/ACK). Porém, a máquina que está executando o Nmap irá enviar um RST para não completar a conexão.

2.6 Ping usando TCP ACK → -PA [ports]

O ping ACK é muito similar ao ping SYN. A diferença é que a flag TCP ACK é marcada ao invés da flag SYN. Tal pacote finge reconhecer dados de uma conexão TCP estabelecida, quando nenhuma conexão existe de fato.

Pode também obter uma lista de portas de destino no mesmo formato. Se um usuário privilegiado tentar isto, o contorno connect() é utilizado. O motivo para oferecer ambas as sondagens ping é maximizar as chances de passar por firewalls.

2.7 Ping usando UDP → -PU [ports]

Este envia um pacote UDP vazio para as portas informadas. O argumento tem o mesmo formato que **-PS** e **-PA**. Uma porta alta incomum é utilizada como padrão porque enviar para portas abertas normalmente é indesejado para este tipo de scan.

Ao bater contra uma porta fechada na máquina-alvo, a sondagem UDP deve causar um pacote ICMP de porta inalcançável como resposta. Isso diz ao Nmap que a máquina está ativa e disponível. Muitos outros tipos de erros ICMP, tais como host/rede inalcançável ou TTL excedido são indicativos de um host inativo ou inalcançável. A falta de resposta também é interpretada desta maneira.

A principal vantagem deste tipo de scan é que ele passa por firewalls e filtros que apenas examinam o TCP.

2.8 Ping usando ARP → -PR

Um dos cenários mais comuns é escanear LAN Ethernet. Na maioria das LANs, especialmente aquelas que utilizam a faixa de endereçamento privativo, abençoado pela RFC1918, a vasta maioria dos endereços IP não são utilizados nunca. Quando o Nmap tenta enviar um pacote IP em estado bruto, tal como ***ICMP echo request***, o OS deve determinar o endereço físico de destino (ARP) correspondente ao IP-alvo, de forma que ele possa endereçar adequadamente o frame ethernet.

O scan ARP encarrega o Nmap e seus algoritmos otimizados de fazer as requisições ARP. E se ele conseguir uma resposta de volta, o Nmap não precisa se preocupar com os pacotes ping baseados em IP.

2.9 Não faz resolução DNS → -n

Diz ao Nmap nunca fazer uma resolução DNS reserva nos endereços IP ativos que ele encontrar.

2.10 Resolução DNS para todos os alvos → -R

Diz ao Nmap para sempre fazer uma resolução DNS reversa nos endereços IP-alvos. Normalmente isto apenas é executado quando uma máquina está ativa.

2.12 Usa resolução DNS do sistema → --system-dns

O Nmap resolve o endereço IP através do envio de pesquisas (queries) diretamente aos servidores de nome configurados em seu host, e então escuta as respostas.

3.Técnicas de escaneamento de portas

A maioria dos tipos de scan está disponível apenas para usuários privilegiados. Isso acontece porque eles enviam e recebem pacotes em estado bruto, o que requer acesso de root em sistemas Unix. Utilizar conta de administrador no Windows é recomendado, embora o Nmap às vezes funcione com usuários sem privilégios nessa plataforma.

3.1 Scan TCP SYN → -sS

O scan SYN é a opção de scan padrão e mais popular por boas razões. Pode ser executada rapidamente, escaneando milhares de portas por segundo em uma rede rápida, não bloqueada por firewalls intrusivos. O scan SYN é relativamente não-obstrusivo e camuflado, uma vez que ele nunca completa uma conexão TCP. Comumente chamado de escaneamento de porta entreaberta porque você não abre uma conexão TCP completamente, apenas envia um pacote SYN e então espera uma resposta. Um SYN/ACK indica que a porta está ouvindo (aberta), enquanto um RST (reset) indica que a porta não está ouvindo. Se nenhuma resposta é recebida, a porta é marcada como filtrada.

3.2 Scan TCP connect→ -sT

Este é quando o scan SYN não é uma opção. Esse é o caso quando o usuário não tem privilégio para criar pacotes em estado bruto ou escanear redes IPv6. Ao invés de criar estes pacotes, o Nmap pede ao OS para estabelecer uma conexão com a máquina e porta alvos enviando uma chamada de sistema connect().

A chamada de sistema completa as conexões nas portas-alvo abertas ao invés de executar o reset de porta entreaberta que o scan SYN faz. Isso não só leva mais tempo e requer mais pacotes para obter a mesma informação, mas também torna mais provável que as máquinas-alvo registrem a conexão.

Um sistema IDS decente irá detectar qualquer um deles, mas a maioria das máquinas não tem esse tipo de sistema de alarme.

Muitos firewalls são configurados para simplesmente descartar pacotes recebidos. O Nmap envia uma solicitação TCP SYN e não recebe nada de volta. Isto indica que a porta está sendo protegida por um firewall e, portanto, a porta é considerada filtrada.

3.3 Scans UDP → -sU

Os serviços UDP são amplamente difundidos. O DNS, o SNMP e o DHCP são três dos mais comuns. O scan UDP funciona enviando um cabeçalho UDP vazio (sem dados) para cada porta almejada. Se um erro ICMP de porta inalcançável é retornado, a porta está fechada. Outros erros do tipo inalcançável marcam a porta filtrada. Ocasionalmente um serviço irá responder com um pacote UDP, provando que está aberto.

Um grande desafio com o escaneamento UDP é fazê-lo rapidamente. Portas abertas e filtradas raramente enviam alguma resposta, deixando o Nmap esgotar o tempo e então efetuar retransmissões para o caso da sondagem ou a resposta ter sido perdida. Portas fechadas costumam enviar de volta um erro ICMP de porta inalcançável.

O Nmap detecta limitações de taxa e diminui o ritmo de acordo para evitar inundar a rede com pacotes inúteis que a máquina-alvo irá descartar.

3.4 Scans TCP Null, FIN e Xmas → -sN | -sF | -sX (respectivamente)

Estes três scans exploram uma brecha sutil na RFC do TCP para diferenciarem entre portas abertas e fechadas. Diz-se que “se a porta [destino] estiver FECHADA… um segmento entrante que não contenha um RST irá causar o envio de um RST como resposta”.

Quando se escaneia sistemas padronizados com o texto desta RFC, qualquer pacote que não contenha os bits SYN, RST ou ACK irá resultar em um RST como resposta, se a porta estiver fechada, e nenhuma resposta se a porta estiver aberta.

- scan null (-sN) não marca nenhum bit, logo, o cabeçalho de flag do TCP é 0
- scan FIN (-sF) marca apenas o bit FIN do TCP
- scan Xmas (-sX) marca as flags FIN, PSH e URG, iluminando o pacote como uma árvore de natal

Esses três tipos de scan são exatamente os mesmos termos de comportamento, exceto pelas flags TCP marcadas nos pacotes de sondagem. Se um pacote RST for recebido, a porta é considerada fechada, e nenhuma resposta significa que está aberta|filtrada.

A principal vantagem desses scans é que eles podem bisbilhotar através de alguns firewalls não-orientados à conexão e de roteadores que filtram pacotes. Outra vantagem é que esses tipos de scan são um pouco mais camuflados do que o scan SYN. A maioria dos produtos IDS modernos podem ser configurados para detectar estes tipos de pacotes.

Diversos sistemas enviam respostas RST para as sondagens independentemente do fato da porta estar aberta ou não. Isso faz com que todas as portas sejam classificadas como fechadas. Este scan realmente funciona contra a maioria dos sistemas baseados em Unix.

A resposta esperada para portas abertas com essas varreduras também é idêntica e muito semelhante à de uma varredura UDP. Se a porta estiver aberta, não haverá resposta ao pacote malformado. Infelizmente, esse também é um comportamento esperado se a porta estiver protegida por um firewall, portanto, as varreduras NULL, FIN e Xmas só identificarão as portas como abertas | filtradas, fechadas ou filtradas. Se uma porta for identificada como filtrada com uma dessas varreduras, geralmente é porque o alvo respondeu com um pacote ICMP inacessível.

Em particular, sabe-se que o Microsoft Windows (e muitos dispositivos de rede Cisco) responde com um RST a qualquer pacote TCP malformado - independentemente de a porta estar realmente aberta ou não. Isso faz com que todas as portas apareçam como fechadas. Dito isto, o objetivo aqui é, obviamente, evadir o firewall.

Muitos firewalls são configurados para descartar pacotes TCP recebidos em portas bloqueadas que possuem o sinalizador SYN definido. Ao enviar solicitações que não contêm o sinalizador SYN, contornamos efetivamente esse tipo de firewall. Embora isso seja bom em teoria, a maioria das soluções IDS modernas são experientes com esses tipos de varredura, portanto, não confie nelas para serem 100% eficazes ao lidar com sistemas modernos.

3.5 Scan TCP ACK → -sA

Este scan nunca determina se uma porta está aberta (ou aberta|filtrada). Ele é utilizado para mapear conjuntos de regras do firewall, determinando se eles são orientados à conexão ou não, e quais portas estão filtradas.

O pacote de sondagem do scan ACK tem apenas a flag ACK marcada. Quando se escaneia sistemas não-filtrados, as portas abertas e fechadas irão devolver um pacote RST. O Nmap então coloca nelas o rótulo não-filtradas, significando que elas estão alcançáveis pelo pacote ACK, mas elas estão abertas ou fechadas é indeterminado.

Portas que não respondem, ou que devolvem certas mensagens de erro ICMP (tipo 3, código 1, 2, 3, 9, 10 ou 13) são rotuladas como filtradas.

3.6 Scan da janela TCP → -sW

Este scan é exatamente o mesmo que o scan ACK, exceto que ele explora um detalhe da implementação de certos sistemas de forma a diferenciar as portas abertas das fechadas, ao invés de simplesmente mostrar não-filtradas quando um RST é devolvido.

Este scan se baseia em um detalhe de implementação de uma minoria de sistemas na Internet, portanto não se pode confiar sempre nele. Sistemas que não suportam isso irão normalmente devolver todas as portas como fechadas.

3.7 Scans do protocolo IP → -sO

Estes scans permitem que você determine quais protocolos IP (TCP, ICMP, IGMP, entre outros) são suportados pelas máquinas-alvo. Isso não é, tecnicamente, um scan de portas. Ainda assim, ele utiliza a opção **-p** para selecionar os números de protocolos a escanear, mostra os resultados dentro do formato normal da tabela de portas e usa o mesmo mecanismo de escaneamento dos métodos de descoberta de portas.

4.Especificações de portas e ordem de scan

Somado a todos os métodos de scan, o Nmap oferece opções para especificar quais portas são escaneadas e se a ordem de escaneamento é aleatória ou sequencial.

4.1 Escaneia apenas as portas especificadas → -p [faixa_portas]

Esta opção permite especificar quais portas você deseja escanear e prevalece sobre o padrão. Números de portas individuais são suportadas, bem como as faixas separadas por um hífen (1-1023). Os valores iniciais e/ou finais da faixa podem ser omitidos, o que faz com que o Nmap use 1 e 65.535, respectivamente.

Você pode especificar **-p-** para escanear as portas de 1 até 65.535. Escanear a porta 0 é permitido se você especificar explicitamente. Quando escanear ambas as

portas TCP e UDP, você pode especificar um protocolo em particular, precedendo os números de portas com T: ou U:

4.2 Scan rápido com portas limitadas → -F

Especifica que você deseja apenas escanear as portas listadas no arquivo *nmap-services* que vem com o Nmap. Isto é muito mais rápido do que escanear todas as portas de um host. Pelo fato desta lista conter tantas as portas TCP, a diferença de velocidade de um scan TCP padrão não é dramática. A diferença pode ser enorme se você especificar seu próprio minúsculo arquivo usando a opção **--datadir**

4.3 Não usa as portas de forma aleatória → -r

Por padrão, o Nmap usa a ordem das portas a serem escaneadas de forma aleatória. Essa técnica de busca aleatória normalmente é desejável, mas pode-se especificar esta flag para um escaneamento de porta sequencial.

5.Detecção de serviços e versão

Quando fizer uma avaliação de vulnerabilidades de sua empresa ou clientes, você realmente deseja saber qual o programa-servidor de correio eletrônico ou de nomes e as versões que estão rodando. Ter um número de versão exato ajuda substancialmente na determinação de quais explorações (exploits) o servidor está vulnerável. A detecção de versão ajuda a obter essa informação.

Depois que as portas TCP e/ou UDP forem descobertas usando qualquer um dos outros métodos de scan, a detecção de versão interroga essas portas para determinar mais informações sobre o que realmente está sendo executado nessas portas.

O Nmap tenta determinar os protocolos de serviços, o nome da aplicação, o número de versão, o nome do host, tipo de dispositivo, a família do OS e às vezes detalhes diversos do tipo, se um servidor X está aberto para conexões, a versão do protocolo SSH ou o nome do usuário do KaZaA.

Quando o Nmap recebe uma resposta de um serviço, mas não consegue encontrá-la em seu banco de dados, ele mostra uma identificação especial e uma URL para que você envie informações se souber com certeza o que está rodando nesta porta.

5.1 Detecção de versão → -sV

Habilita a detecção de versão. Alternativamente, você pode usar a opção **-A** para habilitar tanto a detecção de OS como a detecção de versão

5.2 Não exclui nenhuma porta da detecção de versão → -allports

Por padrão, a detecção de versão pula a porta TCP 9100 por causa de algumas impressoras que imprimem qualquer coisa que seja enviada para essa porta levando a

dezenas de páginas com requisições HTTP. Esse comportamento pode ser alterado modificando-se ou removendo a diretiva Exclude no *nmap-service-probes*, ou pelo comando acima.

5.3 Estabelece a intensidade do scan de versão → --version-intensity

Quando está sendo executado um scan de versão, o Nmap envia uma série de sondagens, cada qual com um valor atribuído de raridade, entre 1 e 9. As sondagens com números baixos são efetivas contra uma ampla variedade de serviços comuns, enquanto as com números mais altos são raramente úteis. Quanto mais alto o número, maiores as chances do serviço ser corretamente identificado, entretanto, scans de alta intensidade levam mais tempo.

6.Detecção de SO

Uma das características mais conhecidas do Nmap é a detecção remota de SO utilizando a identificação da pilha do TCP/IP. O Nmap envia uma série de pacotes TCP e UDP ao host remoto e examina praticamente todos os bits das respostas. Após executar dezenas de testes como a amostragem TCP ISN, suporte e ordenamento das opções do TCP, amostragem IPID e a checagem do tamanho inicial da janela, o Nmap compara os resultados com o banco de dados *nmap-os-fingerprints* com mais de 1500 identificações de OS conhecidas e mostra os detalhes do OS se houver uma correspondência.

Se o Nmap não conseguir identificar o OS da máquina, e as condições forem favoráveis, o Nmap irá fornecer uma URL onde você poderá enviar a identificação se souber com certeza o SO em execução na máquina. A detecção de OS habilita diversos outros testes que usam informações coletadas durante o processo.

6.1 Habilita a detecção de OS → -O

Habilita a detecção de sistema operacional. Alternativamente, você pode usar **-A** para habilitar tanto a detecção de OS quanto a detecção de versão.

7.Evitando e enganando o firewall/IDS

As obstruções de rede, como o firewall, podem tornar o mapeamento de uma rede extremamente difícil. E isso não vai se tornar mais fácil, pois sufocar as sondagens casuais e, frequentemente, o objetivo principal de se instalar esses dispositivos. O Nmap oferece muitas ferramentas para ajudar a entender essas redes complexas, e para verificar que os filtros estão funcionando como esperado. Ele até suporta mecanismo para passar por cima de defesas mal implementadas. Um dos melhores métodos para se entender a postura de segurança de uma rede é tentar derrubá-la.

Além de restringir a atividade de rede, as empresas estão monitorando o tráfego cada vez ais, com sistemas de detecção de intrusão (IDS). Todos os principais IDS vêm com regras designadas para detectar escaneamentos feitos com o Nmap porque os scans são, às vezes, precursores de ataques.

7.1 Fragmenta os pacotes → -f | Usando a MTU especificada → --mtu

A primeira opção faz com que o scan solicitado (incluindo ping) utilize pequenos pacotes IP fragmentados. A ideia é dividir o cabeçalho TCP em diversos pacotes para tornar mais difícil para os filtros de pacotes, os sistemas de detecção de intrusão e outros aborrecimentos, detectar o que você está fazendo.

Você pode especificar o tamanho da quebra com a opção **--mtu**. Não especifique também **-f** se você usar o **--mtu**. A quebra deve ser um múltiplo de 8. Embora os pacotes fragmentados não passem por filtros de pacotes e firewall que enfileirem todos os fragmentos IP, tal como a opção CONFIG_IP_ALWAYS_DEFRAG do kernel do Linux faz, algumas redes não aguentam o impacto no desempenho que isso causa, deixando a opção desabilitada. Outros não conseguem habilitar porque os fragmentos podem seguir por rotas diferentes.

7.2 Disfarça o endereço de origem → -S

Em algumas circunstâncias, o Nmap pode não conseguir determinar o seu endereço de origem. Nesta situação, use **-S** com o endereço IP da interface que você deseja utilizar para enviar os pacotes.

7.3 Use a interface especificada → -e

Diz ao Nmap qual interface deve ser utilizada para enviar e receber pacotes. O Nmap deveria ser capaz de detectar isto automaticamente, mas ele informará se não conseguir.

7.4 Disfarça o número de porta de origem → --source-port [número_porta] | -g [número_porta]

Um administrador que configura um firewall novo, apenas para ser inundado com queixas de usuários ingratos cujas aplicações param de funcionar. Em particular, o DNS pode parar de funcionar porque as respostas DNS UDP de servidores externos não conseguem mais entrar na rede.

Soluções seguras para esses problemas existem, frequentemente na forma de proxies no nível da aplicação ou módulos de firewall para análise de protocolo. Infelizmente também há soluções mais fáceis e inseguras.

Administradores de rede sobrecarregados não são os únicos a caírem nessa armadilha. Diversos produtos foram empacotados com essas regras inseguras.

O Nmap oferece as opções **-g** e **--source-port** (equivalentes) para explorar essas fraquezas. Apenas forneça um número de porta e o Nmap irá enviar pacotes dessa porta onde for possível. O Nmap utiliza números de porta diferentes par que certos testes de detecção de OS funcionem direito, e as requisições DNS ignoram a flag **--source-port** porque o Nmap confia nas bibliotecas de sistema para lidar com isso.

7.5 Acrescenta dados aleatórios nos pacotes enviados → --data-length [value]

Esta opção faz com que o Nmap acrescente o número informado de bytes aleatórios na maioria dos pacotes que envia. Os pacotes de detecção de OS não são afetados, pois a precisão exige consistência das sondagens, mas a maioria dos pacotes de ping e scan de portas funcionam assim.

7.6 Estabelece o valor do campo time-to-live → --ttl [value]

Estabelece que o campo tempo-de-vida dos pacotes enviados terá o valor informado.

-7.7 -randomize-hosts (torna aleatória a ordem dos hosts-alvo)

Informa ao Nmap que ele deve embaralhar cada grupo de, no máximo, 8096 hosts antes de escaneá-los. Isso torna os scans menos óbvios a vários sistemas de monitoramento de rede, especialmente quando você combina isso com as opções de temporização lentas. Se você deseja fazer isso em grupos maiores, aumente o PING_GROUP_SZ no *nmap.h*.

7.8 Disfarça o endereço MAC → --spoof-mac [endereço mac, prefixo, ou nome do fabricante]

Solicita ao Nmap que utilize o endereço MAC informado para todos os frames ethernet em estado bruto que ele enviar. Esta opção implica em **-send-eth** para assegurar que o Nmap realmente envie pacotes no nível ethernet. O MAC fornecido pode assumir diversos formatos. Se for apenas a string “0”, o Nmap irá escolher um MAC completamente aleatório para a sessão. Se a string informada for um número par de dígitos hexa, o Nmap irá usa-la como o MAC. Se menos do que 12 dígitos hexa forem informados, o Nmap preenche o restante dos 6 bytes com valores aleatórios.

7.9 Envia pacotes TCP/UDP com soma de verificação falsa → --badsum

Solicita ao Nmap que utilize uma soma de verificação TCP ou UDP inválida para os pacotes enviados aos hosts.Uma vez que virtualmente todas as pilhas IP do host irão rejeitar esses pacotes, quaisquer respostas recebidas são provavelmente vindas de um firewall ou IDS que nem se incomodou em verificar a soma de verificação. Pode ser usado para determinar a presença de um firewall.

8.Saída (output)

Além de oferecer diversos formatos de saída, o Nmap fornece opções para controlar a verbosidade da saída, bem como as mensagens de depuração. Os tipos de saída podem ser enviados para a saída padrão ou para arquivos, o qual o Nmap pode acrescentar ou então sobrescrever. Arquivos de saída também podem ser utilizados para se retomar scans abortados.

O Nmap torna a saída disponível em cinco formatos diferentes. O padrão é chamado de saída interativa e é enviada para a saída padrão (stdout). Há também a saída normal, similar à interativa exceto pelo fato de mostrar menos informações e alertas sobre a execução uma vez que se espera que seja feita uma análise somente após o scan completar.

Os outros dois tipos de saída são a saída simples para o grep (grepable output) que inclui a maioria das informações de um host-alvo em uma única linha e a saída script kiddie para usuários que se consideram irados.

8.1 Saída normal → -oN

Solicita que a saída normal seja direcionada para o arquivo informado

8.2 Saída em XML → -oX

Solicita que a saída seja direcionada para o arquivo informado. O Nmap inclui uma definição do tipo de documento que permite que os analisadores XML validem a saída em XML do Nmap.

8.3 Saída script kiddie → -oS [especificação arquivo]

É como a saída interativa, com a diferença de ser pós-processada para atender melhor aos “hackers de elite” que antigamente rejeitavam o Nmap devido ao uso consistente de maiúsculas e minúsculas e a grafia correta.

8.4 Saída para o grep → -oG [especificação arquivo]

O formato de saída XML é muito mais poderoso e é bastante adequado para usuários avançados. O XML é um padrão para o qual existem dezenas de excelentes interpretadores (parsers) disponíveis, enquanto que a saída para o grep é um quebra-galho.

É um formato simples que lista cada host em uma linha e pode ser pesquisado de forma trivial, e interpretado por qualquer ferramenta padrão do Unix, como o grep, awk, cut, sed, diff e Perl. A saída para o grep consiste de comentários e linhas-alvo.

8.5 Saída para todos os formatos → -oA [nome_base]

Você pode especificar este comando para armazenar os resultados de scan nos formatos normal, XML e para o grep de uma vez. Eles são armazenados nos arquivos **nome-base.nmap**, **nome-base.xml** e **nome-base.gnmap**, respectivamente. Como na

maioria dos programas, você pode colocar como prefixo aos nomes de arquivos o caminho de um diretório.

9.Opções de verbosidade e depuração (debugging)

9.1 Aumenta o nível de verbosidade → -v

Aumenta o nível de verbosidade, fazendo com que o Nmap mostre mais informações sobre o progresso do scan. Portas abertas são mostradas conforme são encontradas, e estimativas de tempo para o término são fornecidos quando o Nmap acha que um scan irá demorar mais do que alguns minutos.

9.2 Aumenta ou estabelece o nível de depuração → -d [nível]

Se mesmo o modo verboso não fornece dados suficientes para você, o modo de depuração está disponível para inundá-lo com muito mais. Assim como na opção de verbosidade, a depuração é habilitada com uma flag na linha de comando e o nível de depuração pode ser aumentado especificando-a múltiplas vezes. Alternativamente, você pode estabelecer o nível de depuração fornecendo um argumento para o comando (ex: -d9).

9.3 Rastreia pacotes e dados enviados e recebidos → --packet-trace

Faz com que o Nmap mostre um sumário de todos os pacotes enviados ou recebidos. Isto é bastante usado para depuração, mas também é uma forma valiosa para novos usuários entenderem exatamente o que o Nmap está fazendo por baixo dos panos.

9.4 Lista as interfaces e rotas → --iflist

Mostra a lista de interfaces e rotas do sistema conforme detectados pelo Nmap. Isto é útil para depurar problemas de roteamento ou erro de caracterização de dispositivo.

9.5 Registrar os erros/avisos em um arquivo de saída em modo normal → --log-errors

Avisos e erros mostrados pelo Nmap normalmente aparecem apenas na tela deixando quaisquer arquivos de saída com formato normal especificados íntegros. Mas quando você quer realmente ver essas mensagens no arquivo de saída que você especificou, inclua esta opção. As mensagens continuarão a aparecer no modo interativo. Isto não funciona para a maioria dos erros ligados à argumentos inválidos na linha de comando.

10.Opções diversas de saída

10.1 Acrescenta no arquivo de saída, ao invés de sobrepor → --append-output

Quando você especifica um nome de arquivo na flag de formato de saída, esse arquivo é sobreposto por padrão. Se você preferir manter o conteúdo existente do arquivo e acrescentar os novos resultados, especifique este comando. Todos os arquivos de saída especificados na execução do Nmap terão os resultados acrescidos ao invés de sobrepostos.

10.2 Retoma um scan abortado → --resume [nome_arquivo]

O administrador que está rodando o Nmap poderia cancelar um scan por qualquer razão. Reiniciar um scan inteiro do começo pode ser indesejável. Felizmente, se forem mantidas logs normal ou para o grep, o usuário pode pedir que o Nmap continue o escaneamento do alvo que estava verificando quando a execução foi interrompida. Simplesmente use este comando e informe o arquivo de saída normal/para o grep como argumento. Nenhum outro argumento é permitido, pois o Nmap analisa o arquivo de saída e usa os mesmos argumentos especificados anteriormente.

10.3 Habilita o escaneamento IPv6 → -6

Muito embora o IPv6 não ter exatamente se alastrado pelo mundo, seu uso se torna mais significativo em alguns países e a maioria dos sistemas operacionais modernos passam a suportá-lo. Para usar o Nmap com o IPv6, tanto a origem, quanto o alvo de seu scan devem estar configurados para IPv6.

10.4 Opções agressivas de scan → -A

Esta opção habilita opções adicionais avançadas e agressivas.

10.5 Libera a memória antes de terminar → --release-memory

Esta opção é útil apenas para depuração de vazamentos de memória. Ela faz com que o Nmap libere memória alocada pouco antes de encerrar de forma a tornar os vazamentos de memória reais mais fáceis de se ver. Normalmente, o Nmap pula essa parte pois o SO faz isso de qualquer forma no encerramento de um processo

10.6 Assume que o usuário é altamente privilegiado → --privileged

Informa ao Nmap para simplesmente assumir que o alvo tem privilégio suficiente para executar transmissões de sockets em estado bruto, farejar pacotes e operações similares que normalmente requerem privilégio de root em sistemas Unix. Por padrão, o Nmap se encerra se tal operação é solicitada, mas o geteuid() não é zero.