Conteúdo

Sumário das Opções

Este sumário de opções é mostrado quando o Nmap é executado sem argumentos, e a última versão está sempre disponível em http://insecure.org/nmap/data/nmap.usage.txt. Ele ajuda as pessoas a lembrar das opções mais comuns, mas não substitui a documentação mais técnica do restante deste manual. Algumas opções obscuras não estão incluídas aqui.

```
Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0-255.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -P0: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery probes to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes resolve]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver

SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idlescan
  -sO: IP protocol scan
  -b <ftp relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Fast - Scan only the ports listed in the nmap-services file)
  -r: Scan ports consecutively - don't randomize

SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)

OS DETECTION:
  -O: Enable OS detection (try 2nd generation, then 1st if that fails)
  -O1: Only use the old (1st generation) OS detection system
  -O2: Only use the new OS detection system (no fallback)
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:
  Options which take <time> are in milliseconds, unless you append 's'
  (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T[0-5]: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <time>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
```

FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address, prefix, or vendor name>: Spoof your MAC address

OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan results in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use twice for more effect)
  -d[level]: Set or increase debugging level (Up to 9 is meaningful)
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Insecure.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:
  -6: Enable IPv6 scanning
  -A: Enables OS detection and Version detection
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  -V: Print version number
  -h: Print this help summary page.

Especificação de Alvo

Tudo na linha de comando do Nmap que não for uma opção (ou argumento de uma opção) é tratado como uma especificação de um host-alvo. O caso mais simples é especificar um endereço IP como alvo ou um hostname para ser escaneado.

Algumas vezes você pode querer escanear uma rede inteira de hosts adjacentes. Para isso o Nmap suporta o estilo de endereçamento CIDR. Você pode acrescentar /<númerodebits> em um endereço ou hostname e o Nmap irá escanear cada endereço IP para o qual os primeiros <númerosdebits> sejam o mesmo que o IP de referência ou o hostname dado. Por exemplo, 192.168.10.0/24 escanearia os 256 hosts entre 192.168.10.0 (binário: 11000000 10101000 00001010 00000000) e 192.168.10.255 (binário: 11000000 10101000 00001010 11111111), inclusive. 192.168.10.40/24 faria exatamente a mesma coisa. Dado que o host scanme.nmap.org está no endereço IP 205.217.153.62, a especificação scanme.nmap.org/16 escanearia os 65.536 endereços IP entre 205.217.0.0 e 205.217.255.255. O menor valor permitido é /1, que equivale a escanear metade da Internet. O maior valor é 32, que escaneia apenas o host nomeado ou endereço IP porque todos os bits de endereçamento estão fixos.

A notação CIDR é curta mas nem sempre flexível o suficiente. Por exemplo, você pode querer escanear 192.168.0.0/16 mas desejar pular todos os IPs terminados em .0 ou .255 porque eles são normalmente endereços de broadcast. O Nmap suporta isso através de endereçamento por faixa de octeto. Ao invés de especificar um endereço IP normal, você pode especificar uma lista de números separada por vírgulas ou faixa de números para cada octeto. Por exemplo, 192.168.0-255.1-254 irá pular todos os endereços na faixa que terminarem com .0 e/ou .255. Faixas não precisam ser limitadas ao octeto final: o especificador 0-255.0-255.13.37 irá executar um scan em toda a Internet buscando os endereços IP terminados em 13.37. Esse tipo de amostragem ampla pode ser útil em levantamentos e pesquisas da Internet toda.

Endereços IPv6 podem apenas ser especificados utilizando o endereço ou hostname IPv6 completamente qualificado. Faixas CIDR e octetos não são suportados para o IPv6 porque eles raramente são úteis.

O Nmap aceita múltiplas especificações de host na linha de comando, e elas não precisam ser do mesmo tipo. O comando nmap scanme.nmap.org 192.168.0.0/16 10.0.0,1,3-7.0-255 executa o que se espera que dele.

Embora os alvos sejam normalmente especificados na linha de comando, as seguintes opções também estão disponíveis para controlar a seleção de alvos:

-iL <arquivodeentrada> (Entrada à partir de uma lista)

Lê a especificação de alvos à partir de um <arquivodeentrada>. Passar uma lista enorme de hosts na linha de comando é muito ruim, ainda que seja comumente desejável. Por exemplo, seu servidor DHCP pode exportar uma lista de 10.000 endereços correntes em uso que você deseja escanear. Ou talvez você deseje escanear todos os endereços IP exceto aqueles usados para localizar hosts que usam endereços IP estáticos não-autorizados. Simplesmente gere uma lista de hosts a escanear e passe o nome do arquivo para o Nmap como um argumento à opção -iL. As entradas podem estar em qualquer um dos formatos aceitos pelo Nmap na linha de comando (endereço IP, hostname, CIDR, IPv6, ou faixas de octetos). Cada entrada deve ser separada por um ou mais espaços em branco, tabulações ou quebra de linhas. Você pode especificar um hífen (-) como nome de arquivo se quiser que o Nmap leia os nomes de hosts da entrada padrão (standard input) ao invés de um arquivo.

-iR <número de hosts> (Escolhe alvos aleatórios)

Para levantamentos na Internet toda e outras pesquisas, você pode querer escolher alvos de forma aleatória. O argumento <número de hosts> diz ao Nmap quantos IPs ele deverá gerar. IPs indesejáveis, tais como aqueles de certas redes privativas, multicast e faixas de endereços não-alocadas são automaticamente desconsideradas. O argumento 0 (zero) pode ser especificado caso deseje um scan sem fim. Tenha em mente que alguns administradores de rede "torcem o nariz" para scans não-autorizados de suas redes e podem reclamar. Use esta opção por sua conta e risco! Se você estiver realmente entediado em uma tarde chuvosa, tente o comando nmap -sS -PS80 -iR 0 -p 80 para localizar servidores web aleatórios para navegar.

--exclude <host1[,host2][,host3],...> (Exclui hosts/redes)

Especifica uma lista de alvos, separados por vírgula, a serem excluídos do scan mesmo que façam parte da faixa de rede especificada. A lista que você fornece utiliza a sintaxe normal do Nmap, portanto ela pode incluir nomes de hosts, blocos de rede CIDR, faixas de octetos, etc. Isso pode ser útil quando a rede que você deseja escanear inclui servidores de missão crítica intocáveis, sistemas que reajam contrariamente a escaneamento de portas ou sub-redes administradas por outras pessoas.

--excludefile <arquivo_exclusão> (Exclui a lista do arquivo)

Oferece a mesma funcionalidade que a opção --exclude, exceto que os alvos a excluir são fornecidos em um <"arquivo separado"> , delimitados por quebra de linhas, espaço em branco ou tabulação, ao invés de na linha de comando.

Descoberta de Hosts

Um dos primeiros passos em qualquer missão de reconhecimento de uma rede é reduzir um conjunto (às vezes enorme) 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. É claro que o que torna um host interessante depende muito do propósito do scan. Administradores de rede podem estar apenas interessados em hosts que executam um determinado serviço, enquanto os auditores de segurança podem se importar com cada dispositivo que possuir um endereço IP. Um administrador pode se sentir à vontade em usar o ping ICMP para localizar os hosts na rede interna, enquanto um profissional externo de análise de vulnerabilidades (penetration tester) pode utilizar um conjunto diversificado de dezenas de sondagens em uma tentativa de burlar as restrições do firewall.

As necessidades para o descobrimento de host são muito diversas e, por isso, o Nmap oferece uma ampla variedade de opções para customizar as técnicas utilizadas. A descoberta de host às vezes é chamada de ping scan, mas ela vai muito além dos simples pacotes ICMP de echo request associados com a ferramenta onipresente conhecida como ping. Os usuários podem pular a etapa do ping inteiramente com uma lista de scan (-sL) ou desabilitanto o ping (-P0), ou enfrentar a rede com combinações arbitrárias de sondagens multi-portas TCP SYN/ACK, UDP e ICMP. O objetivo dessas sondagens é solicitar respostas que mostrem que um endereço IP está realmente ativo (é utilizado por um host ou dispositivo de rede). Em muitas redes, apenas uma pequena percentagem dos endereços IP está ativa em um dado momento. Isso é particularmente comum com o espaço de endereçamento privativo abençoado pela RFC1918 como, por exemplo, 10.0.0.0/8. Essa rede tem 16 milhões de IPs, mas eu já a vi sendo utilizado em empresas com menos de mil máquinas. A descoberta de hosts pode encontrar essas máquinas escassamente alocadas em um mar de endereços IP.

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. Uma exceção a isso é que um scan ARP é utilizado para cada alvo localizado na rede ethernet local. Para usuários Unix sem privilégios, com shell, um pacote SYN é enviado ao invés do ack utilizando a chamada de sistema connect(). Esses valores padrão equivalem às opções -PA -PE. Esta descoberta de host freqüentemente é suficiente para escanear redes locais, mas um conjunto de sondagens mais abrangentes é recomendado para auditoria de segurança.

As opções -P* (que selecionam tipos de ping) podem ser combinadas. Você pode aumentar as chances de penetrar em um firewall rígido enviando muitos tipos de sondagens, utilizando diferentes portas/flags TCP e códigos ICMP. Note também que a descoberta por ARP (-PR) é feita por padrão contra alvos na rede ethernet local mesmo que você especifique outras opções -P* , porque é quase sempre mais rápida e eficiente.

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. Isto é verdade mesmo que você especifique tipos de busca não-padronizadas de hosts, tais como sondagens UDP (-PU). Leia sobre a opção -sP para saber como executar apenas uma descoberta de hosts, ou utilize -P0 para pular a descoberta de hosts e escanear as portas de todos os hosts-alvo. As seguintes opções controlam a descoberta de hosts:

-sL (Scan Listagem)

O scan 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. Ainda é surpreendente a quantidade de informações úteis que simples nomes de hosts podem dar. Por exemplo, fw.chi.playboy.com é o firewall do escritório de Chicago da Playboy Enterprises. Nmap também reporta o número total de endereços IP ao final. O scan listagem é um bom teste de sanidade para assegurar que você está com a lista correta de endereços IP dos seus alvos. Se os hosts mostrarem nomes de domínios que você não reconhece, vale a pena investigar melhor para evitar scanear a rede da empresa errada.

Uma vez que a idéia é apenas mostrar uma lista dos hosts-alvos, as opções de funcionalidade de nível mais alto tais como scan de portas, detecção de SO, ou scan utilizando ping, não podem ser combinadas com esta opção. Se você deseja desabilitar o scan utilizando ping enquanto executa funções de nível elevado, leia a opção -P0.

-sP (Scan usando Ping)

Esta opção diz ao Nmap para somente executar um scan usando o ping (descoberta de hosts), e então mostrar os hosts disponíveis que responderam ao scan. Nenhum teste adicional (tais como escaneamento de portas e deteção de SO) é executado. Isto é um pouco mais intrusivo que o scan listagem, e pode ser usado para os mesmos propósitos. Permite um reconhecimento leve de uma rede-alvo sem chamar muita atenção. Saber quantos hosts estão ativos é mais valioso para invasores que a lista fornecida pelo scan listagem com cada endereço IP e seu nome de host.

Administradores de sistemas frequentemente acham esta opção valiosa. Ela pode ser facilmente utilizada para contar o número de máquinas disponíveis em uma rede ou monitorar a disponibilidade dos servidores. Isto é normalmente chamado de varredura com ping (ping sweep), e é mais confiável do que fazer um ping em um endereço de broadcast, pois muitos hosts não respondem a pesquisas com broadcast.

A opção -sP envia um ICMP echo request e um pacote TCP para a porta 80 por padrão. Quando executada por um usuário sem privilégios, um pacote SYN é enviado (usando uma chamada connect()) para a porta 80 no alvo. Quando um usuário privilegiado tenta escanear alvos na rede ethernet local, requisições ARP (-PR) são utilizadas, a menos que --send-ip tenha sido especificado. A opção -sP pode ser combinada com qualquer um dos tipos de sondagens de descobrimento (as opções -P* , excluindo -P0) para maior flexibilidade. Se qualquer uma dessas opções de tipos de sondagens e número de porta for utilizada, as sondagens padrão (ACK e echo request) são sobrepostas. Quando firewalls restritivos estão posicionados entre o host de origem que executa o Nmap e a rede-alvo, utilizar essas técnicas avançadas é recomendado. Do contrário, hosts podem ser perdidos quando o firewall ignorar as sondagens ou as respostas delas.

-P0 (Sem ping)

Esta opção pula completamente o estágio de descoberta do Nmap. Normalmente o Nmap utiliza este estágio para determinar as máquinas ativas para escaneamento mais agressivo. Por padrão, o Nmap apenas executa sondagens agressivas tais como escaneamento de portas, detecção de versões, ou detecções do SO contra hosts que foram verificados como ativos. Desabilitar a descoberta de hosts com -P0 faz com que o Nmap teste as funções de escaneamento solicitadas contra todos os endereços IP alvos especificados. Portanto se um espaço de endereçamento alvo do tamanho de uma classe B (/16) for especificado na linha de comando, todos os 65.536 endereços IP serão escaneados. O segundo caracter da opção -P0 é um zero e não a letra O. A descoberta de hosts apropriada é desconsiderada como no scan listagem, mas ao invés de parar e mostrar a lista de alvos, o Nmap continua a executar as funções solicitadas como se cada alvo IP estivesse ativo.

-PS [listadeportas] (Ping usando TCP SYN)

Esta opção envia um pacote TCP vazio com a flag SYN marcada. A porta de destino padrão é a 80 (configurada em tempo de compilação pela variável DEFAULT_TCP_PROBE_PORT no nmap.h), mas uma porta alternativa pode ser especificada como um parâmetro. Até uma lista de portas separadas por vírgula pode ser especificada (p.ex. -PS22,23,25,80,113,1050,35000), nesse caso as sondagens serão tentadas contra cada porta em paralelo.

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 de a porta estar aberta, o alvo irá dar o segundo passo do cumprimento-de-três-vias (3-way-handshake) do TCP respondendo com um pacote TCP SYN/ACK TCP. A máquina executando o Nmap então derruba a conexão recém-nascida respondendo com um RST ao invés de enviar um pacote ACK que iria completar o cumprimento-de-três-vias e estabelecer uma conexão completa. O pacote RST é enviado pelo kernel da máquina que está executando o Nmap em resposta ao SYN/ACK inesperado, e não pelo próprio Nmap.

O Nmap não se importa se a porta está aberta ou fechada. Tanto a resposta RST ou SYN/ACK discutidas anteriormente dizem ao Nmap se o hosts está disponível e responsivo.

Em caixas UNIX, apenas o usuário privilegiado root é capaz, normalmente, de enviar e receber pacotes TCP em estado bruto. Para usuários não privilegiados um contorno é automaticamente empregado em concordância com a chamada de sistema connect() iniciada contra cada porta-alvo. Isso tem o efeito de enviar um pacote SYN ao host alvo, em uma tentativa de se estabelecer uma conexão. Se o connect() retornar com sucesso rápido ou com uma falha ECONNREFUSED, a pilha TCP subjacente deve ter recebido um SYN/ACK ou RST e o host é marcado como disponível. Se a tentativa de conexão for deixada largada até que um timeout ocorra, o host é marcado como indisponível. Esse contorno também é usado para conexões IPv6, pois o suporte a construção de pacotes IPv6 em estado bruto ainda não está disponível no Nmap.

-PA [listadeportas] (Ping usando TCP ACK)

O ping usando TCP ACK é muito similar ao recém-discutido ping usando SYN. A diferença, como você poderia imaginar, é que a flag TCP ACK é marcada ou invés da flag SYN. Tal pacote ACK finge reconhecer dados de uma conexão TCP estabelecida, quando nenhuma conexão existe de fato. Então os hosts remotos deveriam sempre responder com pacotes RST, revelando sua existência no processo.

A opção -PA utiliza a mesma porta padrão que a sondagem SYN (80) e pode também obter uma lista de portas destino no mesmo formato. Se um usuário privilegiado tenta isto, ou se um alvo IPv6 é especificado, o contorno connect() discutido anteriormente é utilizado. Esse contorno é imperfeito pois o connect() está realmente enviando um pacote SYN ao invés de um ACK.

O motivo para oferecer ambas as sondagens ping, que utilizam SYN e ACK, é maximizar as chances de passar por firewalls. Muitos administradores configuram roteadores e outros firwalls simples para bloquear pacotes SYN entrantes exceto aqueles destinados a serviços públicos como o site web da empresa ou servidor de correio eletrônico. Isso evita as demais conexões entrantes na organização, permitindo aos usuários fazer conexões desobstruidas à Internet. Essa aproximação não-orientada à conexão (non-stateful ou stateless) consome uns poucos recursos no firewall/roteador e é amplamente suportada por filtros de hardware e software. O firewall de software Netfilter/iptables do Linux oferece a conveniência da opção --syn para implementar essa abordagem stateless. Quando regras stateless do firewall tais como essas são implementadas, sondagens de ping usando SYN (-PS) muito provavelmente serão bloqueadas quando forem enviadas à portas fechadas. Em tais casos, a sondagem ACK se destaca pois ela simplesmente passa por essas regras.

Outro tipo comum de firewall utiliza regras orientadas a conexão que descartam pacotes inesperados. Esta característica era encontrada inicialmente apenas em firewalls de alto-nível, embora tenha se tornado mais comum com o passar dos anos. O sistema Netfilter/iptables do Linux suporta esta característica através da opção --state, que categoriza os pacotes baseados no estado da conexão. Uma sondagem SYN tem maiores chances de funcionar contra um sistema assim, pois pacotes ACK inesperados são normalmente reconhecidos como falsos e descartados. Uma solução para esse dilema é enviar ambas as sondagens SYN e ACK especificando -PS e -PA.

-PU [listadeportas] (Ping usando UDP)

Outra opção de descoberta de hosts é o ping usando UDP, que envia um pacote UDP vazio (a menos que --data-length seja especificado) para as portas informadas. O argumento "listadeportas" tem o mesmo formato que os discutidos anteriormente nas opções -PS e -PA. Se nenhuma porta for especificada, o padrão é 31338. Esse padrão pode ser configurado em tempo de compilação alterando DEFAULT_UDP_PROBE_PORT no nmap.h. Uma porta alta incomum é utilizada como padrão porque enviar para portas abertas normalmente é indesejado para este tipo particular 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 dessa forma. Se uma porta aberta é alcançada, a maioria dos serviços simplesmente ignoram o pacote vazio e falham em retornar qualquer resposta. É por isso que a porta de sondagem padrão é 31338, que pouco provavelmente estará em uso. Uns poucos serviços, tal como o chargen, irá responder a um pacote UDP vazio, e com isso revelará ao Nmap que a máquina está disponível.

A principal vantagem deste tipo de scan é que ele passa por firewalls e filtros que apenas examinam o TCP. Por exemplo, uma vez eu tive um roteador broadband sem-fio Linksys BEFW11S4. A interface externa desse dispositivo filtrava todas as portas TCP por padrão, mas as sondagens UDP ainda causavam mensagens de porta inalcançável, entregando assim o dispositivo.

-PE; -PP; -PM (Tipos de Ping do ICMP)

Além dos tipos incomuns de descoberta de hosts TCP e UDP discutidos anteriormente, o Nmap pode enviar os pacotes-padrão que normalmente são enviados pelo onipresente programa ping. O Nmap envia um pacote ICMP do tipo 8 (echo request) ao endereço IP alvo, esperando como resposta um tipo 0 (Echo Reply) do host disponível. Infelizmente para muitos exploradores de rede, muitos hosts e firewalls atualmente bloqueiam esses pacotes, ao invés de responder como é requerido pela RFC 1122. Por essa razão, scans puramente ICMP são raramente confiáveis o suficiente contra alvos desconhecidos na Internet. Mas para administradores de sistemas

monitorando uma rede interna eles podem ser uma abordagem prática e eficiente. Utilize a opção -PE para ativar esse comportamento echo request.

Embora o echo request seja a pesquisa padrão de um ping ICMP, o Nmap não pára aqui. A padronização do ICMP (RFC 792) também especifica timestamp request, information request, e pacotes address mask request como códigos 13, 15, e 17, respectivamente. Apesar do propósito ostensivo dessas pesquisas seja obter informações tais como a máscara do endereço e hora corrente, eles podem ser facilmente utilizados para descoberta de hosts. Um sistema que responda está ativo e disponível. O Nmap não implementa atualmente os pacotes de requisição de informações, pois eles não são amplamente suportados. A RFC 1122 insiste que "um host NÃO DEVERIA implementar essas mensagens". Pesquisas de marcação de hora (Timestamp) e máscara de endereço podem ser enviadas com as opções -PP e -PM , respectivamente. Uma resposta timestamp reply (código ICMP 14) ou uma resposta address mask reply (código 18) revela que o host está disponível. Essas duas pesquisas podem ser valiosas quando os administradores bloqueiam pacotes echo request especificamente e esquecem que outras pesquisas ICMP podem ser usadas com o mesmo propósito.

-PR (Ping usando ARP)

Um dos cenários de uso mais comuns do Nmap é escanear a 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 um ICMP echo request, o sistema operacional deve determinar o endereço físico de destino (ARP) correspondente ao IP-alvo de forma que ele possa endereçar adequadamente o frame ethernet. Isso normalmente é lento e problemático, pois os sistemas operacionais não foram escritos com a expectativa de que precisariam fazer milhões de requisições ARP contra hosts indisponíveis em um curto período de tempo.

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 nem se preocupar com os pacotes ping baseados em IP, uma vez que ele já sabe que o host está ativo. Isso torna o scan ARP muito mais rápido e mais confiável que os scans baseados em IP. Portanto isso é feito por padrão quando se escaneia hosts ethernet que o Nmap detecta estarem posicionados em uma rede ethernet local. Mesmo se tipos diferentes de ping (tais como -PI ou -PS) seja especificados, o Nmap usa o ARP no lugar para cada um dos alvos que estiverem na mesma LAN. Se você não quiser de forma nenhuma fazer um scan ARP, especifique --send-ip.

-n (Não faça resolução DNS)

Diz ao Nmap para nunca fazer uma resolução DNS reversa nos endereços IP ativos que ele encontrar. Uma vez que o DNS é normalmente lento, isso acelera as coisas.

-R (resolução DNS para todos os alvos)

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

--system-dns (Usa a resolução DNS do sistema)

Por padrão, 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. Muitas das pesquisas (dezenas) são executadas em paralalo para um melhor desempenho. Especifique esta opção se desejar utilizar a resolução DNS do seu sistema (um endereço IP por vez, através da chamada getnameinfo()). Isto é mais lente e raramente útil, a não ser que haja um bug no código de DNS do Nmap -- por favor, entre em contato conosco se for o caso. A resolução DNS do sistema é sempre usada em escaneamento IPv6.

--dns-servers <servidor1[,servidor2],...> (Servidores a utilizar para a pesquisa DNS reversa)

Por padrão o Nmap irá tentar determinar os seus servidores DNS (para a resolução DNS reversa) através do arquivo resolv.conf (UNIX) ou do registry (Win32). Opcionalmente você pode usar esta opção para especificar servidores alternativos. Esta opção não é honrada se você estiver usando --system-dns ou um escaneamento IPv6. Utilizar múltiplos servidores DNS é, normalmente, mais rápido e mais furtivo do que pesquisar apenas em um servidor. O melhor desempenho é frequentemente obtido especificando-se todos os servidores que tem autoridade sobre a faixa de endereços IP.

Fundamentos do Escaneamento de Portas

Embora o Nmap tenha crescido em funcionalidade ao longo dos anos, ele começou como um eficiente scanner de portas, e essa permanece sua função principal. O simples comando nmap <alvo> escaneia mais de 1660 portas TCP no host <alvo>. Embora muitos scanner de portas tenham tradicionalmente agrupado todas as portas nos estados aberto ou fechado, o Nmap é muito mais granular. Ele divide as portas em seis estados: aberto(open), fechado(closed),filtrado(filtered), não-filtrado(unfiltered), open|filtered, ou closed|filtered.

Esses estados não são propriedades intrínsecas da porta, mas descrevem como o Nmap as vê. Por exemplo, um scan do Nmap da mesma rede como alvo pode mostrar a porta 135/tcp como aberta, enquanto um scan ao mesmo tempo com as mesmas opções, à partir da Internet poderia mostrar essa porta como filtrada.

Os seis estados de porta reconhecidos pelo Nmap

aberto (open)

Uma aplicação está ativamente aceitando conexões TCP ou pacotes UDP nesta porta. Encontrar esse estado é freqüentemente o objetivo principal de um escaneamento de portas. Pessoas conscientes sobre a segurança sabem que cada porta aberta é um convite para um ataque. Invasores e profissionais de avaliação de segurança querem explorar as portas abertas, enquanto os administradores tentam fechar ou proteger com firewalls sem bloquear usuários legítimos. Portas abertas são também interessantes para scans não-relacionados à segurança pois mostram os serviços disponíveis para utilização na rede.

fechado (closed)

Uma porta fechada está acessível (ela recebe e responde a pacotes de sondagens do Nmap), mas não há nenhuma aplicação ouvindo nela. Elas podem ser úteis para mostrar que um host está ativo em um determinado endereço IP (descoberta de hosts, ou scan usando ping), e como parte de uma deteção de SO. Pelo fato de portas fechadas serem alcançáveis, pode valer a pena escanear mais tarde no caso de alguma delas abrir. Os administradores deveriam considerar o bloqueio dessas portas com um firewall. Então elas apareceriam no estado filtrado, discutido a seguir.

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 de um dispositivo firewall dedicado, regras de roteador, ou um software de firewall baseado em host. Essas 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 proibida administrativamente), mas os filtros que simplesmente descartam pacotes sem responder são bem mais comuns. Isso força o Nmap a tentar diversas vezes só para o caso de a sondagem ter sido descartada por congestionamento da rede ao invés de filtragem. Isso reduz a velocidade do scan dramaticamente.

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, tal como scan Window, scan Syn, ou scan FIN, podem ajudar a responder se a porta está aberta.

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 sabe-se com certeza se a porta está aberta ou se está sendo filtrada. Os scans UDP, IP Protocol, FIN, Null, e Xmas classificam portas desta forma.

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.

Técnicas de Escaneamento de Portas

Como um novato executando um reparo automotivo, posso brigar por horas tentando usar minhas ferramentas rudimentares (martelo, fita adesiva, grifo, etc.) nas tarefas. Quando eu falho miseravelmente e reboco minha lata-velha para um mecânico de verdade ele invariavelmente pesca aqui e ali em um enorme baú de ferramentas até pegar a coisa perfeita que torna a tarefa uma brincadeira. A arte de escanear portas é similar. Os experts entendem as dezenas de técnicas de escaneamento e escolhem as que são apropriadas (ou uma combinação) para uma dada tarefa. Usuários inexperientes e script kiddies, por outro lado, tentam resolver todos os problemas com o scan SYN padrão. Uma vez que o Nmap é gratuito, a única barreira para a maestria em escaneamento de portas é o conhecimento. Isso certamente é melhor que no mundo automotivo, onde pode ser necessário uma grande habilidade para determinar que você precisa de um compressor de molas e então você tem que pagar milhares de dólares por um.

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 a conta de administrador no Windows é recomendado, embora o Nmap às vezes funcione com usuários sem privilégios nessa plataforma quando o WinPcap foi carregado no SO. Requerer privilégio de root era uma séria limitação quando o Nmap foi lançado em 1997, pois muitos usuários apenas tinham acesso a contas de shell compartilhadas. Agora o mundo é diferente. Computadores estão mais baratos, muito mais pessoas tem acesso direto e

permanente à Internet, e computadores de mesa Unix (incluindo Linux e MAC OS X) são comuns. Uma versão para o Windows do Nmap se encontra disponível atualmente, permitindo que se rode em muito mais computadores de mesa. Por todas essas razões, os usuários tem menos necessidade de executar o Nmap à partir de contas de shell compartilhadas e limitadas. Isso é muito bom pois as opções privilegiadas tornam o Nmap muito mais poderoso e flexível.

Embora o Nmap tente produzir resultados precisos, tenha em mente que todas as deduções são baseadas em pacotes devolvidos pelas máquinas-alvo (ou firewalls na frente delas). Tais hosts podem ser não-confiáveis e enviar respostas com o propósito de confundir ou enganar o Nmap. Muito mais comum são os hosts não-de-acordo-com-a-rfc que não respondem como deveriam às sondagens do Nmap. As sondagens FIN, Null e Xmas são particularmente suscetíveis a esse problema. Tais questões são específicas de determinados tipos de scan e portanto são discutidos nas entradas individuais de cada um dos tipos.

Esta seção documenta as dezenas de técnicas de escaneamento de portas suportadas pelo Nmap. Apenas um método pode ser utilizado de cada vez exceto que um scan UDP (-sU) pode ser combinado com qualquer um dos tipos de scan TCP. Como uma ajuda para a memória, as opções dos tipos de escaneamento de portas estão no formato -s<C>, onde <C> é um caracter proeminente no nome do scan, normalmente o primeiro. A única exceção a essa regra é para o scan depreciado FTP bounce (-b). Por padrão, o Nmap executa um scan SYN, embora ele substitua por um scan connect se o usuário não tiver os privilégios adequados para enviar pacotes em estado bruto (requer acesso de root no UNIX) ou se alvos IPv6 forem especificados. Dos scans listados nesta seção, os usuários não privilegiados podem apenas executar os scans connect e ftp bounce.

-sS (scan TCP SYN)

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. Ele também trabalha contra qualquer pilha TCP padronizada ao invés de depender de idiossincrasias de plataformas específicas como os scans Fin/Null/Xmas, Maimon e Idle fazem. Ele também permite uma diferenciação limpa e confiável entre os estados aberto (open), fechado (closed), e filtrado (filtered).

Esta técnica é freqüentemente chamada de escaneamento de porta entreaberta (half-open scanning), porque você não abre uma conexão TCP completamente. Você envia um pacote SYN, como se fosse abrir uma conexão real e então espera uma resposta. Um SYN/ACK indica que a porta está ouvindo (aberta), enquanto um RST (reset) é indicativo de uma não-ouvinte. Se nenhuma resposta é recebida após diversas retransmissões, a porta é marcada como filtrada. A porta também é marcada como filtrada se um erro ICMP de inalcançável é recebido (tipo 3, código 1,2, 3, 9, 10, ou 13).

-sT (scan TCP connect)

O scan TCP connect é o scan padrão do TCP quando o scan SYN não é uma opção. Esse é o caso quando o usuário não tem privilégios para criar pacotes em estado bruto ou escanear redes IPv6. Ao invés de criar pacotes em estado bruto como a maioria dos outros tipos de scan fazem, o Nmap pede ao sistema operacional para estabelecer uma conexão com a máquina e porta alvos enviando uma chamada de sistema connect(). Essa é a mesma chamada de alto nível que os navegadores da web, clientes P2P, e a maioria das outras aplicações para rede utilizam para estabelecer uma conexão. É parte da interface de programação conhecida como API de Sockets de Berkeley. Ao invés de ler as respostas em pacotes em estado bruto diretamente dos fios, o Nmap utiliza esta API para obter informações do estado de cada tentativa de conexão.

Quando um scan SYN está disponível é normalmente a melhor escolha. O Nmap tem menos controle sobre a chamada de alto nível connect() do que sobre os pacotes em estado bruto, tornando-o menos eficiente. 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 serviços na maioria dos sistema Unix irão acrescentar uma nota no syslog, e às vezes uma mensagem de erro obscura, quando o Nmap se conecta e então fecha a conexão sem enviar nenhum dado. Serviços verdadeiramente patéticos irão travar quando isso acontecer, embora isso seja incomum. Um administrador que vê um punhado de tentativas de conexão nos registros vindos de um único sistema deveria saber que foi escaneado com connect().

-sU (scans UDP)

Embora os serviços mais populares na Internet trafeguem sobre o protocolo TCP, os serviços UDP são amplamente difundidos. O DNS, o SNMP, e o DHCP (registrados nas portas 53, 161/162, e 67/68) são três dos mais comuns. Pelo fato do escaneamento UDP ser normalmente mais lento e mais difícil que o TCP, alguns auditores de segurança ignoram essas portas. Isso é um erro, pois serviços UDP passíveis de exploração são bastante comuns e invasores certamente não ignoram o protocolo inteiro. Felizmente o Nmap pode ajudar a inventariar as portas UDP.

O scan UDP é ativado com a opção -sU. Ele pode ser combinado com um tipo de escaneamento TCP como o scan SYN (-sS) para averigüar ambos protocolos na mesma execução.

O scan UDP funciona enviando um cabeçalho UDP vazio (sem dados) para cada porta almejada. Se um erro ICMP de porta inalcançável (tipo 3, código 3) é retornado, a porta está fechada. Outros erros do tipo inalcançável (tipo 3, códigos 1, 2, 9, 10, ou 13)

marcam a porta como filtrada. Ocasionalmente um serviço irá responder com um pacote UDP, provando que está aberta. Se nenhuma resposta é recebida após as retransmissões, a porta é classificada como aberta|filtrada. Isso significa que a porta poderia estar aberta, ou talvez que filtros de pacotes estejam bloqueando a comunicação. Scans de versões (-sV) podem ser utilizados para ajudar a diferenciar as portas verdadeiramente abertas das que estão filtradas.

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 (time out) e então efetuar retransmissões para o caso de a sondagem ou a resposta ter sido perdida. Portas fechadas são, normalmente, um problema ainda maior. Elas costumam enviar de volta um erro ICMP de porta inalcançável. Mas, ao contrário dos pacotes RST enviados pelas portas TCP fechadas em resposta a um scan SYN ou connect, muitos hosts limitam a taxa de mensagens ICMP de porta inalcançável por padrão. O Linux e o Solaris são particularmente rigorosos quanto a isso. Por exemplo, o kernel 2.4.20 do Linux limita a quantidade de mensagens de destino inalcançável a até uma por segundo (no net/ipv4/icmp.c).

O Nmap detecta a limitação de taxa e diminui o ritmo de acordo para evitar inundar a rede com pacotes inúteis que a máquina-alvo irá descartar. Infelizmente, um limite como o do Linux de um pacote por segundo faz com que um scan de 65.536 portas leve mais de 18 horas. Idéias para acelerar o escaneamento UDP incluem escanear mais hosts em paralelo, fazer um scan rápido apenas das portas mais comuns primeiro, escanear por detrás de um firewall, e utilizar --host-timeout para pular os hosts lentos.

-sN; -sF; -sX (scans TCP Null, FIN, e Xmas)

Esses três tipos de scan (existem outras opções, possíveis com a opção --scanflags descrita na próxima seção) exploram uma brecha sutil na RFC do TCP para diferenciarem entre portas abertas e fechadas. A página 65 diz que "se a porta [destino] estiver FECHADA .... um segmento entrante que não contenha um RST irá causar o envio de um RST como resposta." Então a página seguinte discute os pacotes enviados à portas abertas sem os bits SYN, RST ou ACK marcados, afirmando que: "é pouco provável que você chegue aqui, mas se chegar, descarte o segmento, e volte."

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. Contanto que nenhum desses três bits estejam incluídos, qualquer combinação dos outros três (FIN, PSH e URG) é válida. O Nmap explora isso com três tipos de scan:

scan Null (-sN)
Não marca nenhum bit (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 em termos de comportamento, exceto pelas flags TCP marcadas no pacotes de sondagem. Se um pacote RST for recebido, a porta é considerada fechada, e nenhuma resposta significa que está aberta|filtrada. A porta é marcada como filtrada se um erro ICMP do tipo inalcançável (tipo 3, código 1, 2, 3, 9, 10, ou 13) for recebido.

A vantagem principal desses tipos de scan 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. Mas, não conte com isso -- a maioria dos produtos IDS modernos podem ser configurados para detectá-los. O maior problema é que nem todos os sistemas seguem a RFC 793 ao pé-da-letra. 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. A maioria dos sistemas operacionais que fazem isso são Microsoft Windows, muitos dispositivos Cisco, BSDI, e o IBM OS/400. Esse scan realmente funciona contra a maioria dos sistemas baseados em Unix. Outro ponto negativo desses scans é que eles não conseguem diferenciar portas abertas de alguns tipos de portas filtradas, deixando você com a resposta abera|filtrada.

-sA (scan TCP ACK)

Esse scan é diferente dos outros discutidos até agora pelo fato de que ele nunca determina se uma porta está aberta (ou mesmo 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 (a menos que você use --scanflags). 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 (unfiltered), significando que elas estão alcançáveis pelo pacote ACK, mas se 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.

-sW (scan da Janela TCP)

Scan da Janela 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 sempre mostrar não-filtrada quando um RST é devolvido. Ele faz isso examinando o campo Janela TCP (TCP Window) do pacote RST devolvido. Em alguns sistemas, as portas abertas usam um valor positivo de tamanho de janela (mesmo para pacotes RST), enquanto que as portas fechadas tem um valor igual a zero. Então, ao invés de sempre mostrar uma porta como não-filtrada quando se recebe um RST de volta, o scan da Janela mostra a porta como aberta ou fechada se o valor da Janela TCP no reset for positivo ou zero, respectivamente.

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. É claro que é possível que a máquina realmente não tenha nenhuma porta aberta. Se a maioria das portas escaneadas estiver fechada mas uns poucos números de portas comuns (tais como 22, 25, 53) estão filtrados, o sistema muito provavelmente está vulnerável. De vez em quando, os sistemas irão mostrar exatamente o comportamento oposto. Se o seu scan mostrar 1000 portas abertas e 3 fechadas ou filtradas, então essas três podem muito bem ser as verdadeiramente abertas.

-sM (scan TCP Maimon)

O scan Maimon recebeu o nome de seu descobridor, Uriel Maimon. Ele descreveu a técnica na Phrack Magazine, edição 49 (Novembro de 1996). O Nmap, que incluiu essa técnica, foi lançado duas edições mais tarde. A técnica é exatamente a mesma que os scans Null, FIN e Xmas, exceto que a sondagem é FIN/ACK. De acordo com a RFC 793 (TCP), um pacote RST deveria ser gerado em resposta a tal sondagem se a porta estiver aberta ou fechada. Entretanto, Uriel notou que muitos sistemas derivados do BSD simplesmente descartavam o pacote se a porta estivesse aberta.

--scanflags (scan TCP Personalizado)

Usuários verdadeiramente avançados do Nmap não precisam se limitar aos tipos de scans enlatados oferecidos. A opção --scanflags permite que você desenhe seu próprio scan permitindo a especificação de flags TCP arbitrárias. Deixe sua imaginação correr solta enquanto dribla sistemas de detecção de intrusão, cujos fabricantes apenas olharam rapidamente a página man do Nmap adicionando regras específicas!

O argumento do --scanflags pode ser um valor numérico da marca (flag) como o 9 (PSH e FIN), mas usar nomes simbólicos é mais fácil. Apenas esprema alguma combinação de URG, ACK, PSH, RST, SYN, e FIN. Por exemplo, --scanflags URGACKPSHRSTSYNFIN marca tudo, embora não seja muito útil para escaneamento. A ordem em que essas marcas são especificadas é irrelevante.

Além de especificar as marcas desejadas, você pode especificar um tipo de scan TCP (como o -sA ou -sF). Esse tipo-base diz ao Nmap como interpretar as respostas. Por exemplo, um scan SYN considera nenhuma-resposta como uma indicação de porta filtrada, enquanto que um scan FIN trata a mesma como aberta|filtrada. O Nmap irá se comportar da mesma forma que o tipo de scan-base escolhido, exceto que ele irá usar as marcas TCP que você especificar. Se você não escolher um tipo-base, o scan SYN é utilizado.

-sI <hostzumbi[:portadesondagem]> (scan Idle)

Este método avançado de scan permite um scan TCP realmente cego das portas do alvo (significando que nenhum pacote é enviado para o alvo do seu endereço IP real). Ao invés disso, um ataque canal-lateral (side-channel) explora a previsível geração de seqüencia de ID, conseqüencia da fragmentação do IP, no host zumbi, para juntar informações sobre as portas abertas no alvo. Sistemas IDS irão mostrar o scan como se viessem da máquina zumbi que você especificou (que deve estar ativa e obedecer a alguns critérios). Este tipo fascinante de scan é complexo demais para se descrever completamente aqui, neste guia de referência, então eu escrevi e postei um trabalho informal com detalhes completos em http://nmap.org/book/idlescan.html.

Além de ser extraordinariamente camuflado (devido à sua natureza cega), este tipo de scan permite mapear relações de confiança baseadas em IP entre máquinas. A listagem de portas mostra as portas abertas da perspectiva do host zumbi. Portanto você pode tentar escanear algo usando vários zumbis que você acha que podem ser confiáveis (via regras de roteador/filtro de pacotes).

Você pode adicionar o sinal "dois-pontos", seguido do número da porta, ao nome do host zumbi se quiser sondar uma porta em particular no zumbi, verificando as mudanças de IPID. Do contrário o Nmap irá utilizar a porta que ele normalmente usa por padrão para pings tcp (80).

-sO (Scans do protocolo IP)

Scans do Protocolo IP permitem que você determine quais protocolos IP (TCP, ICMP, IGMP, etc.) são suportados pelas máquina-alvo. Isso não é, tecnicamente, um scan de portas, pois ele varia os números do protocolo IP ao invés dos números de portas TCP e UDP. 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. Portanto ele é parecido o suficiente com um scan de portas e por isso pertence à este lugar.

Além de ser útil de seu jeito, o scan de protocolo mostra o poder do software de código aberto. Embora a idéia fundamental seja bastante simples, eu não havia pensado em adicioná-la e nem havia recebido nenhuma solicitação para essa funcionalidade. Então, no verão de 2000, Gerhard Rieger concebeu a idéia, escreveu uma excelente alteração (patch) implementando-a, e a enviou para a lista de discussão nmap-hackers. Eu incorporei a alteração na árvore do Nmap e lancei uma nova versão no dia seguinte. Poucos produtos de software comercial tem usuários entusiasmados o suficiente para desenhar e contribuir com melhorias!

O scan de protocolo funciona de uma forma similar a um scan UDP. Ao invés de ficar repetindo alternando o campo de número de porta de um pacote UDP, ele envia cabeçalhos de pacote IP e faz a repetição alternando o campo de protocolo IP de 8 bits. Os cabeçalhos normalmente estão vazios, sem conter dados, e nem mesmo contendo o cabeçalho apropriado do suposto protocolo. As três exceções são o TCP, o UDP e o ICMP. Um cabeçalho de protocolo apropriado para estes é incluído, uma vez que alguns sistemas não os enviarão caso não tenham, e porque o Nmap tem as funções para criá-los Ao invés de observar as mensagens de erro ICMP de porta inalcançável, o scan de protocolo fica de olho nas mensagens ICMP de protocolo inalcançável. Se o Nmap recebe qualquer resposta de qualquer protocolo do host-alvo, o Nmap marca esse protocolo como aberto. Um erro ICMP de protocolo não-alcançável (tipo 3, código 2) faz com que o protocolo seja marcado como fechado. Outros erros ICMP do tipo inalcançável (tipo 3, código 1, 3, 9, 10, ou 13) fazem com que o protocolo seja marcado como filtrado (embora eles provem, ao mesmo tempo, que o ICMP está aberto). Se nenhuma resposta for recebida após as retransmissões, o protocolo é marcado como aberto|filtrado.

-b <host para relay de ftp> (Scan de FTP bounce)

Uma característica interessante do protocolo FTP (RFC 959) é o suporte à conexões denominadas proxy ftp. Isso permite que um usuário conecte-se a um servidor FTP, e então solicite que arquivos sejam enviados a um terceiro servidor. Tal característica é sujeita a abusos em diversos níveis, por isso a maioria dos servidores parou de suportá-la. Um dos abusos permitidos é fazer com que o servidor FTP escaneie as portas de outros hosts. Simplesmente solicite que o servidor FTP envie um arquivo para cada porta interessante do host-alvo. A mensagem de erro irá descrever se a porta está aberta ou não. Esta é uma boa forma de passar por cima de firewalls porque os servidores FTP de empresas normalmente são posicionados onde tem mais acesso a outros hosts internos que os velhos servidores da Internet teriam. O Nmap suporta o scan de ftp bounce com a opção -b. Ela recebe um argumento no formato <nomedousuário>:<senha>@<servidor>:<porta>. <Servidor> é o nome ou endereço IP de um servidor FTP vulnerável. Assim como em uma URL normal, você pode omitir <nomedousuário>:<senha>, neste caso as credenciais de login anônimo (usuário: anonymous senha:-wwwuser@) serão usados. O número da porta (e os dois-pontos) podem ser omitidos, e então a porta FTP padrão (21) no <servidor> será utilizada.

Esta vulnerabilidade espalhou-se em 1997 quando o Nmap foi lançado, mas foi corrigida amplamente. Servidores vulneráveis ainda estão por aí, então pode valer a pena tentar se tudo o mais falhar. Se passar por cima de um firewall é o seu objetivo, escaneie a rede-alvo procurando por uma porta 21 aberta (ou mesmo por qualquer serviço FTP se você escanear todas as portas com a detecção de versão), então tente um scan bounce usando-as. O Nmap irá dizer se o host é vulnerável ou não. Se você estiver apenas tentando encobrir suas pegadas, você não precisa (e, na verdade, não deveria) limitar-se a hosts na rede-alvo. Antes de sair escaneando endereços aleatórios na Internet, procurando por servidores FTP, considere que os administradores de sistemas podem não apreciar o seu abuso nos servidores deles.

Especificação de Portas e Ordem de Scan

Somado a todos os métodos de scan discutidos anteriormente, o Nmap oferece opções para especificar quais portas são escaneadas e se a ordem de escaneamento é aleatória ou sequencial. Por padrão, o Nmap escaneia todas as portas até, e incluindo, 1024, bem como portas com numeração alta listadas no arquivo the nmap-services para o(s) protocolo(s) escaneados.

-p <faixa de portas> (Escaneia apenas as portas especificadas)

Esta opção especifica quais portas que você deseja escanear e prevalece sobre o padrão. Números de portas individuais são suportadas, bem como as faixas separadas por um hífen (p.ex.: 1-1023). Os valores iniciais e/ou finais da faixa podem ser omitidos, o que faz com que o Nmap use 1 e 65535, respectivamente. Portanto, você pode especificar -p- para escanear as portas de 1 até 65535. Escanear a porta zero é permitido se você especificar explicitamente. Para o escaneamento do protocolo IP (-sO), esta opção especifica os números dos protocolos que você deseja escanear (0-255).

Quando escanear ambas as portas TCP e UDP, você pode especificar um protocolo em particular, precedendo os números de portas com T: ou U:. O qualificador dura até que você especifique um novo qualificador. Por exemplo, o argumento -p U:53,111,137,T:21-25,80,139,8080 escanearia as portas UDP 53, 111 e 137, bem como as portas TCP listadas. Note que para escanear ambas as portas UDP e TCP, você tem que especificar -sU e pelo menos um tipo de scan TCP (tal como -sS, -sF ou -sT). Se nenhum qualificador de protocolo for informado, os números de portas serão acrescentados à todas as listas de protocolos.

-F (Scan Rápido (portas limitadas))

Especifica que você deseja apenas escanear as portas listadas no arquivo nmap-services que vem com o nmap (ou o arquivo de protocolos para o -sO). Isto é muito mais rápido do que escanear todas as 65535 portas de um host. Pelo fato desta lista conter tantas

portas TCP (mais de 1200), a diferença de velocidade de um scan TCP padrão (cerca de 1650 portas) não é dramática. A diferença pode ser enorme se você especificar seu próprio minúsculo arquivo nmap-services usando a opção --datadir.

-r (Não usa as portas de forma aleatória)

Por padrão, o Nmap usa a ordem das portas a serem escaneadas de forma aleatória (exceto aquelas portas normalmente certamente acessíveis que são movidas próximas ao início por motivos de eficiência). Essa técnica de busca aleatória normalmente é desejável, mas você pode especificar -r para um escaneamento de portas sequencial.

Detecção de Serviço e Versão

Aponte o Nmap para uma máquina remota e ele poderá lhe dizer que as portas 25/tcp, 80/tcp e 53/udp estão abertas. Utilizar o banco de dados nmap-services, com cerca de 2.200 serviços bastante conhecidos, do Nmap iria relatar que aquelas portas provavelmente correspondem a um servidor de correio eletrônico (SMTP), a um servidor de páginas web (HTTP) e a um servidor de nomes (DNS) respectivamente. Essa pesquisa normalmente é precisa -- a grande maioria de daemons escutando na porta TCP 25 é, de fato, de servidores de correio eletrônico. Entretanto, você não deveria apostar a sua segurança nesta informação! As pessoas podem e executam serviços em portas estranhas.

Mesmo que o Nmap esteja certo, e o servidor hipotético acima esteja executando os serviços SMTP, HTTP e DNS, isso não é informação o bastante. Quando fizer uma avaliação de vulnerabilidades (ou mesmo um simples inventário da rede) 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 esta 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 banco de dados nmap-service-probes do Nmap contém sondagens para pesquisar diversos serviços e expressões de acerto (match expressions) para reconhecer e destrinchar as respostas. O Nmap tenta determinar os protocolos de serviços (p.ex.: ftp, ssh, telnet, http), o nome da aplicação (p.ex.: ISC Bind, Apache httpd, Solaris telnetd), o número da versão, o nome do host, tipo de dispositivo (p.ex.: impressora, roteador), a família do SO (p.ex.: Windows, Linux) 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. É claro que a maioria dos serviços não fornece todas essas informações. Se o Nmap foi compilado com o suporte ao OpenSSL, ele irá se conectar aos servidores SSL para deduzir qual o serviço que está escutando por trás da camada criptografada. Quando os serviços RPC são descobertos, o "amolador" de RPC (RPC grinder) do Nmap (-sR) é automaticamente utilizado para determinar o nome do programa RPC e o número da versão. Algumas portas UDP são deixadas no estado aberta|filtrada depois que scan de porta UDP não consegue determinar se a porta está aberta ou filtrada. A detecção de versão irá tentar provocar uma resposta dessas portas (do mesmo jeito que faz com as portas abertas), e alterar o estado para aberta se conseguir. Portas TCP do tipo aberta|filtrada são tratadas da mesma forma. Note que a opção -A do Nmap habilita a detecção de versão, entre outras coisas. Um trabalho documentando o funcionamento, uso e customização da detecção de versão está disponível em http://insecure.org/nmap/vscan/.

Quando o Nmap recebe uma resposta de um serviço mas não consegue encontrá-la em seu banco de dados, ele mostra uma identificação (fingerprint) especial e uma URL para que você envie informações se souber com certeza o que está rodando nessa porta. Por favor, considere dispor de alguns minutos para mandar essa informação de forma que sua descoberta possa beneficiar a todos. Graças a esses envios, o Nmap tem cerca de 3.000 padrões de acerto para mais de 350 protocolos, tais como o smtp, ftp, http, etc.

A detecção de versão é habilitada e controlada com as seguintes opções:

-sV (detecção de versão)

Habilita a detecção de versão, conforme discutido acima. Alternativamente, você pode usar a opção -A para habilitar tanto a detecção de SO como a detecção de versão.

--allports (Não exclui nenhuma porta da detecção de versão)

Por padrão, a detecção de versão do Nmap 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, requisições de sessões SSL binárias, etc. Esse comportamento pode ser alterado modificando-se ou removendo a diretiva Exclude no nmap-service-probes, ou você pode especificar --allports para escanear todas as portas independente de qualquer diretiva Exclude.
--version-intensity <intensidade> (Estabelece a intensidade do scan de versão)

Quando está executando um scan de versão (-sV), 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 altos são raramente úteis. O nível de intensidade especifica quais sondagens devem ser utilizadas. Quando mais alto o

número, maiores as chances de o serviço ser corretamente identificado. Entretanto, scans de alta intensidade levam mais tempo. A intensidade deve estar entre 0 e 9. O padrão é 7. Quando uma sondagem é registrada na porta-alvo através da diretiva nmap-service-probes ports, essa sondagem é tentada independentemente do nível de intensidade. Isso assegura que as sondagens DNS sempre serão tentadas contra qualquer porta 53 aberta, e a sondagem SSL será realizada contra a 443, etc.
--version-light (Habilita o modo leve (light))

Esse é um apelido conveniente para --version-intensity 2. Esse modo leve torna o escaneamento de versão muito mais rápido, mas é ligeiramente menos provável que identifique os serviços.
--version-all (Tenta simplesmente todas as sondagens)

Um apelido para --version-intensity 9, assegurando que todas as sondagens sejam tentadas contra cada porta.
--version-trace (Monitora as atividades do scan de versão)

Isto faz com que o Nmap mostre informações de depuração extensivas sobre o que o escaneamento de versão está fazendo. É um sub-conjunto do que você obteria com --packet-trace.

-sR (Scan RPC)

Este método trabalha em conjunto com os vários métodos de escaneamento de portas do Nmap. Ele pega todas as portas TCP/UDP descobertas no estado aberta e inunda-as com comandos NULL do programa SunRPC, em uma tentativa de determinar se elas são portas RPC e, se forem, quais programas e números de versão elas mostram. Dessa forma você pode obter efetivamente a mesma informação que o rpcinfo -p mesmo se o portmapper do alvo estiver atrás de um firewall (ou protegido por TCP wrappers). Chamarizes não funcionam ainda com o scan RPC. Isso é habilitado automaticamente como parte do scan de versão (-sV) se você o solicitar. Como a detecção de versão inclui isso e é muito mais abrangente, o -sR raramente é necessário.

Detecção de SO

Uma das características mais conhecidas do Nmap é a detecção remota de SO utilizando a identificação da pilha (stack fingerprinting) 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 SO conhecidas e mostra os detalhes do SO se houver uma correspondência. Cada identificação inclui uma descrição textual livre do SO e uma classificação que fornece o nome do fabricante (p.ex.: Sun), SO base (p.ex.: Solaris), geração do SO (p.ex.: 10) e tipo de dispositivo (genérico, roteador, switch, console de jogo, etc.).

Se o Nmap não conseguir identificar o SO da máquina, e as condições forem favoráveis (p.ex.: pelo menos uma porta aberta e uma porta fechada foram encontradas), o Nmap irá fornecer uma URL onde você poderá enviar a identificação se souber (com certeza) o SO em execução na máquina. Fazendo isso, você contribui para a gama de sistemas operacionais conhecidos pelo Nmap e, com isso, ele será mais preciso para todos.

A detecção de SO habilita diversos outros testes que usam as informações coletadas durante o processo. Um deles é a medição de uptime, que utiliza a opção timestamp do TCP (RFC 1323) para supor quando uma máquina foi reiniciada pela última vez. Isso apenas é mostrado para as máquinas que fornecem essa informação. Outro é a Classificação de Previsibilidade da Seqüencia do TCP. Ele mede aproximadamente o grau de dificuldade de se estabelecer uma conexão TCP forjada contra um host remoto. É útil para se explorar relações de confiança baseadas no IP de origem (rlogin, filtros de firewall, etc.) ou para ocultar a origem de um ataque. Esse tipo de enganação (spoofing) raramente é executada hoje em dia, mas muitas máquinas ainda estão vulneráveis a ele. O número de dificuldade real é baseado em amostragens estatísticas e pode variar. Normalmente é melhor usar a classificação em inglês, do tipo “worthy challenge” (um desafio que vale a pena) ou “trivial joke” (uma piada, muito fácil). Isso só é mostrado na saída normal do modo verbose (-v). Quando o modo verbose é habilitado juntamente com o -O, a Geração de Seqüencia IPID também é mostrada. A maioria das máquinas é classificada como “incremental” , o que significa que elas incrementam o campo ID no cabeçalho IP para cada pacote que envia. Isso torna-as vulnerável a diversos ataques avançados de levantamento e forjamento de informações.

Um trabalho documentando o funcionamento, utilização e customização da detecção de SO está disponível em mais de uma dezena de línguas em http://insecure.org/nmap/osdetect/.

A detecção de SO é habilitada e controlada com as seguintes opções:

-O (Habilita a detecção de SO)

Habilita a deteção de SO, como discutido acima. Alternativamente, você pode usar -A para habilitar tanto a detecção de SO quanto a detecção de versão.
--osscan-limit (Limitar a detecção de SO a alvos promissores)

A detecção de SO é bem mais eficiente se ao menos uma porta TCP aberta e uma fechada for encontrada. Escolha esta opção e o Nmap não irá nem tentar a detecção de SO contra hosts que não correspondam a este critério. Isso pode economizar um tempo considerável, particularmente em scans -P0 contra muitos hosts. Isso só importa quando a detecção de SO é solicitada através de -O ou -A.
--osscan-guess; --fuzzy (Resultados de tentativas de detecção de SO)

Quano o Nmap não é capaz de detectar uma correspondência exata de SO, às vezes ele oferece possibilidades aproximada. A correspondência tem que ser muito próxima para o Nmap fazer isso por padrão. Qualquer uma dessas opções (equivalentes) tornam as tentativas do Nmap mais agressivas. O Nmap ainda assim irá dizer quando uma correspondência imperfeita é mostrada e o nível de confiança (porcentagem) de cada suposição.

Temporização (Timing) e Desempenho

Uma das minhas prioridades mais altas no desenvolvimento do Nmap tem sido o desempenho. Um scan padrão (nmap <hostname>) de um host em minha rede local leva apenas um quinto de segundo. Isso mal dá tempo de piscar o olho, mas esse tempo aumenta conforme você está escaneando dezenas ou centenas de milhares de hosts. Além disso, certos tipos de scan, como o escaneamento UDP ou a detecção de versão, aumentam o tempo de escaneamento substancialmente. Da mesma forma algumas configurações de firewall fazem o mesmo, particularmente quando limitam a taxa de resposta. Embora o Nmap se utilize de paralelismo e muitos outros algoritmos avançados para acelerar esses scans, o usuário tem o controle final sobre como o Nmap executa. Usuários avançados elaboram comandos do Nmap cuidadosamente para obter apenas as informações que importam, sempre se preocupando com as restrições de tempo.

Técnicas para melhorar os tempos de scan incluem omitir testes não-críticos e atualizar até a versão mais recente do Nmap (melhorias de desempenho são feitas freqüentemente). Otimizar os parâmetros de tempo também podem fazer uma grande diferença. Essas opções estão listadas abaixo.

Algumas opções aceitam um parâmetro de tempo. É especificado em milissegundos por padrão, embora você possa acrescentar ‘s’, ‘m’ ou ‘h’ ao valor para especificar segundos, minutos ou horas. Dessa forma, os argumentos --host-timeout arguments 900000, 900s e 15m fazem a mesma coisa.

--min-hostgroup <númerodehosts>; --max-hostgroup <númerodehosts> (Ajuste dos tamanhos dos grupos de scan paralelos)

O Nmap tem a habilidade de fazer um scan de portas ou de versões em múltiplos hosts em paralelo. O Nmap faz isso dividindo a faixa de endereços IP-alvo em grupos, e então escaneando um grupo de cada vez. No geral, grupos maiores são mais eficientes. A contrapartida é que os resultados dos hosts não pode ser fornecido até que o grupo inteiro tenha terminado. Portanto, se o Nmap começou com um tamanho de grupo igual a 50, o usuário não receberia nenhum relatório (exceto pelas atualizações mostradas no modo verbose) até que os primeiros 50 hosts tivessem completado.

Por padrão, o Nmap assume um compromisso para resolver esse conflito. Ele começa com um tamanho de grupo pequeno, igual a cinco, para que os primeiros resultados venham rápido, e então aumenta o tamanho até que chegue em 1024. O número padrão exato depende das opções fornecidas. Por questões de eficiência, o Nmap usa tamanhos de grupo maiores para o UDP ou para scans TCP com poucas portas.

Quando o tamanho de grupo máximo é especificado com --max-hostgroup, o Nmap nunca irá exceder esse tamanho. Especifique um tamanho mínimo com --min-hostgroup e o Nmap irá tentar manter o tamanho dos grupos acima desse nível. O Nmap pode ter que usar tamanhos menores do que você especificou, se não houverem hosts-alvo suficientes restantes em uma dada interface, para completar o mínimo especificado. Ambos podem ser configurados para manter o tamanho do grupo dentro de uma faixa específica, embora isso raramente seja desejado.

O uso primário destas opções é especificar um tamanho de grupo mínimo grande de forma que o scan completo rode mais rapidamente. Uma escolha comum é 256 para escanear uma rede em blocos de tamanho Classe C. Para um scan com muitas portas, exceder esse número não irá ajudar muito. Para scans com poucos números de portas, um tamanho de grupo de hosts de 2048 ou mais pode ser útil.

--min-parallelism <numprobes>; --max-parallelism <numprobes> (Ajuste da paralelização das sondagens)

Estas opções controlam o número total de sondagens que podem estar pendentes para um grupo de hosts. Elas são usadas para o escaneamento de portas e para a descoberta de hosts. Por padrão, o Nmap calcula um paralelismo ideal e constantemente atualizado baseado no desempenho da rede. Se os pacotes estiverem sendo descartados, o Nmap reduz o ritmo e libera menos sondagens pendentes. O número de sondagens ideal aumenta vagarosamente conforme a rede se mostre mais confiável. Estas opções estabelecem limites mínimo e máximo nessa variável. Por padrão, o paralelismo ideal pode cair até 1 se a rede se mostrar não-confiável e subir até diversas centenas em condições perfeitas.

O uso mais comum é estabelecer --min-parallelism em um número maior que 1 para melhorar a velocidade dos scans de hosts ou redes com desempenho ruim. Esta é uma opção arriscada para se ficar brincando pois configurar um valor alto demais pode afetar a

precisão. Configurar isso também reduz a habilidade do Nmap de controlar o paralelismo dinamicamente baseado nas condições da rede. Um valor igual a dez pode ser razoável, embora eu só ajuste esse valor como última alternativa.

A opção --max-parallelism às vezes é configurada para evitar que o Nmap envie aos hosts mais do que uma sondagem por vez. Isso pode ser útil em conjunto com --scan-delay (discutido mais tarde), embora esta última normalmente sirva bem ao propósito por si só. --min-rtt_timeout <tempo>, --max_rtt-timeout <tempo>, --initial-rtt-timeout <tempo> (Ajuste de tempo de expiração (timeouts) das sondagens)

O Nmap mantém um valor de tempo de expiração (timeout) de execução para determinar quanto tempo ele deve esperar por uma resposta de uma sondagem antes de desistir ou retransmitir essa sondagem. Isso é calculado com base nos tempos de resposta de sondagens anteriores. Se a latência da rede se mostrar significativa e variável, esse tempo de expiração pode subir para diversos segundos. Ele também começa com um nível conservador (alto) e pode ficar desse jeito por um tempo, enquanto o Nmap escaneia hosts não-responsivos.

Especificar valores --max-rtt-timeout e --initial-rtt-timeout mais baixos que o padrão pode reduzir o tempo de scan significativamente. Isso é particularmente verdadeiro para scans sem ping (-P0), e para aqueles contra redes bastante filtradas. Mas não se torne muito agressivo. O scan pode acabar levando mais tempo se você especificar um valor tão baixo que muitas sondagens irão expirar o tempo e serem retransmitidas enquanto a resposta ainda está em trânsito.

Se todos os hosts estão em uma rede local, 100 milissegundos é um valor de --max-rtt-timeout razoavelmente agressivo. Se houver roteamento envolvido, faça um ping de um host da rede primeiro com o utilitário ICMP ping, ou com um formatador de pacotes customizados como o hping2, que pode passar por um firewall mais facilmente. Descubra o tempo máximo de round trip em dez pacotes, mais ou menos. Coloque o dobro desse valor em --initial-rtt-timeout e o triplo ou quádruplo para o --max-rtt-timeout. Normalmente eu não configuro o rtt máximo abaixo de 100ms, não importa quais os tempos de ping. Eu também não excedo o valor 1000ms.

--min-rtt-timeout é uma opção raramente utilizada que poderia ser útil quando uma rede é tão não-confiável que mesmo o padrão do Nmap é muito agressivo. Considerando que o Nmap apenas reduz o tempo de expiração para um valor mínimo quando a rede parece ser confiável, esta necessidade não é comum e deveria ser reportada à lista de discussão nmap-dev como um bug.

--max-retries <númerodetentativas> (Especifica o número máximo de retransmissões de sondagens de scan de portas)

Quando o Nmap não recebe nenhuma resposta a uma sondagem de escaneamento de portas, isso pode significar que a porta está filtrada. Ou talvez a sondagem ou a resposta simplesmente se perdeu na rede. Também é possível que o host-alvo tenha habilitado uma limitação de tráfego que tenha bloqueado temporariamente a resposta. Então o Nmap tenta novamente retransmitindo a sondagem inicial. Se o Nmap perceber que a confiabilidade da rede está baixa, ele poderá tentar muitas vezes ainda, antes de desistir de uma porta. Embora isso beneficie a exatidão, isso também aumenta o tempo de escaneamento. Quando o desempenho é crítico, os escaneamentos podem ser acelerados através da limitação do número de retransmissões permitidas. Você pode até especificar --max-retries 0 para evitar qualquer retransmissão, embora isto seja raramente recomendado.

O normal (sem nenhum padrão -T) é permitir dez retransmissões. Se a rede aparentar ser confiável e os hosts-alvo não estiverem limitando o tráfego, o Nmap normalmente fará apenas uma retransmissão. Portanto, a maioria dos escaneamentos de alvos não serão sequer afetados com a redução do --max-retries para um valor baixo, como por exemplo três. Tais valores podem acelerar significativamente o escaneamento de hosts lentos (com limitação de tráfego). Você normalmente perde alguma informação quando o Nmap desiste das portas rapidamente, embora isso seja preferível a permitir que o --host-timeout expire e você perca todas as informações sobre o alvo.

--host-timeout <tempo> (Desiste de hosts-alvo lentos)

Alguns hosts simplesmente levam tempo demais para serem escaneados. Isso pode ser causado por um hardware ou software de rede com fraco desempenho ou pouco confiável, limitação na taxa dos pacotes ou por um firewall restritivo. Os poucos hosts mais lentos de todos os hosts escaneados podem acabar sendo responsáveis pela maior parte do tempo total gasto com o scan. Às vezes é melhor cortar fora o prejuízo e pular esses hosts logo no início. Especifique a opção --host-timeout com o valor máximo de tempo que você tolera esperar. Eu normalmente especifico 30m para ter certeza de que o Nmap não gaste mais do que meia hora em um único host. Note que o Nmap pode estar escaneando outros hosts ao mesmo tempo em que essa meia hora desse único host está correndo, então não é uma perda de tempo total. Um host que expira o tempo é pulado. Nenhum resultado de tabela de portas, detecção de SO ou detecção de versão é mostrado para esse host.

--scan-delay <tempo>; --max-scan-delay <tempo> (Ajusta o atraso entre sondagens)

Esta opção faz com que o Nmap aguarde um tempo determinado entre cada sondagem enviada a um dado host. Isto é particularmente útil no caso de limitação de taxas de transferência. Máquinas Solaris (entre muitas outras) irão normalmente responder à pacotes de sondagens de scans UDP com apenas uma mensagem ICMP por segundo. Qualquer número maior que isso, enviado pelo Nmap, será um desperdício. Um --scan-delay de 1s irá manter uma taxa de transferência baixa. O Nmap tenta detectar a limitação de taxa e ajusta o atraso no scan de acordo, mas não dói especificar explicitamente se você já sabe qual a taxa que funciona melhor.

Quando o Nmap ajusta o atraso no scan aumentando para tentar igualar com a limitação na taxa de transferência, o scan fica consideravelmente mais lento. A opção --max-scan-delay especifica o maior atraso que o Nmap irá permitir. Estabelecer um valor muito baixo pode levar à uma retransmissão de pacotes inútil e à possíveis portas perdidas, quando o alvo utiliza limitação rígida de taxa de transferência.

Outro uso do --scan-delay é para evitar os sistemas de prevenção e detecção de intrusão (IDS/IPS) baseados em limites.
--defeat-rst-ratelimit

Muitos hosts usam há bastante tempo a limitação de taxa de transferência para reduzir o número de mensagens de erro ICMP (tais como os erros de porta-inalcançavel) enviados. Alguns sistemas agora aplicam limitações de taxa similares aos pacotes RST (reset) que eles geram. Isso pode tornar o Nmap consideravelmente mais lento pois o obriga a ajustar seu tempo de forma a refletir essas limitações de taxa. Você pode dizer ao Nmap para ignorar essas limitações de taxa (para scans de porta como o Scan SYN que não trata portas que não respondem como abertas) especificando --defeat-rst-ratelimit.

Utilizar esta opção pode reduzir a precisão, pois algumas portas irão aparecer como não-respondendo porque o Nmap não esperou tempo suficiente para uma resposta RST com taxa limitada. No caso de um scan SYN, o "não-respondendo" resulta na porta sendo rotulada como filtrada ao invés de no estado fechada que vemos quando os pacotes RST são recebidos. Esta opção é útil quando você se importa apenas com as portas abertas e distinguir entre portasfechadas e filtradas não vale o tempo extra.

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> (Estabelece um padrão de temporização)

Embora os controles de temporização de ajuste fino discutidos nas seções anteriores sejam poderosos e efetivos, algumas pessoas os consideram confusos. Ainda mais, escolher os valores apropriados pode, às vezes, tomar mais tempo do que o próprio scan que você está tentando otimizar. Por isso, o Nmap oferece uma aproximação mais simples, com seis padrões de temporização. Você pode especificá-los com a opção -T e os números (0 - 5) ou os nomes. Os nomes de padrões são paranóico (paranoid, 0), furtivo (sneaky, 1), educado (polite, 2), normal (3), agressivo (agressive, 4) e insano (insane, 5). Os dois primeiros são para evitar um IDS. O modo educado (ou polido), diminui o ritmo de escaneamento para usar menos banda e recursos da máquina alvo. O modo normal é o padrão e, portanto, -T3 não faz nada. O modo agressivo acelera os scans assumindo que você está em uma rede razoavelmente rápida e confiável. Finalmente, o modo insano assume que você está em uma rede extraordinariamente rápida ou está disposto a sacrificar alguma precisão pela velocidade.

Esses padrões permitem que o usuário especifique o quão agressivo desejam ser, ao mesmo tempo que deixam o Nmap escolher os valores de temporização exatos. Os padrões também fazem ajustes pequenos na velocidade onde ainda não existem opções para controle de ajuste fino. Por exemplo, -T4 proibe que o atraso dinâmico de escaneamento exceda 10ms para portas TCP e -T5 corta esse valor para 5 milissegundos. Padrões podem ser utilizados em conjunto com controles de ajuste fino e esses controles que você especificar irão ter precedência sobre o padrão de temporização do parâmetro. Eu recomendo usar -T4 quando escanear redes razoavelmente modernas e confiáveis. Mantenha essa opção mesmo que você adicione controles de ajuste fino, de forma que você possa se beneficiar com as pequenas otimizações extras que ela habilita.

Se você tiver uma conexão ethernet ou de banda-larga decente, eu recomendaria sempre utilizar -T4. Algumas pessoas adoram o -T5 embora seja agressivo demais para o meu gosto. As pessoas às vezes especificam -T2 porque acham que diminui a probabilidade de travar os hosts ou porque elas se consideram educadas no geral. Normalmente elas não percebem o quão lento o -T Polite realmente é. Esses scans podem levar dez vezes mais tempo que um scan padrão. Travamento de máquinas e problemas com a banda são raros com as opções de temporização padrão (-T3) e, portanto, eu normalmente as recomendo para escaneadores precavidos. Omitir a detecção de versão é bem mais eficaz do que ficar brincando com os valores de temporização para reduzir esses problemas.

Embora o -T0 e o -T1 possam ser usados para evitar alertas no IDS, eles irão leva muito mais tempo para escanear milhares de máquinas ou portas. Para um scan tão amplo, prefira estabelecer os valores exatos de temporização que você precisa ao invés de depender dos valores "engessados" de -T0 e -T1.

O principal efeito de T0 é serializar o scan de forma que apenas uma porta é escaneada por vez, e então, aguardar cinco minutos entre o envio de cada sondagem. T1 e T2 são similares mas aguardam apenas 15 segundos e 0,4 segundos, respectivamente, entre as sondagens. T3 é o comportamento padrão do Nmap, que inclui o paralelismo. T4 faz o mesmo que --max-rtt-timeout 1250 --initial-rtt-timeout 500 --max_retries 6 e estabelece o atraso máximo de scan TCP em 10 milissegundos. T5 faz o mesmo que --max-rtt-timeout 300 --min-rtt-timeout 50 --initial-rtt-timeout 250 --max-retries 2 --host-timeout 15m e estabelece o atraso máximo de scan TCP em 5ms.

Evitando e enganando o Firewall/IDS

Muitos pioneiros da Internet vislumbraram uma rede mundial aberta com um espaço de endereçamento IP universal que permitisse conexões virtuais entre quaisquer dois nós. Isso permite que os hosts atuem como verdadeiros semelhantes, servindo e obtendo informações uns dos outros. As pessoas poderiam acessar seus computadores domésticos do trabalho, mudando os ajustes do controle de climatização ou abrindo as portas para convidados. Essa visão de conectividade universal foi sufocada pela falta de espaço de endereçamento e preocupações com a segurança. No início dos anos 1990, as empresas começaram a instalar firewalls para o propósito claro de reduzir a conectividade. Rede enormes foram isoladas da Internet-sem-fronteiras por proxies de aplicativos,

tradução de endereçamento de rede (network address translation) e filtros de pacotes. O fluxo irrestrito de informações deu a vez à regulamentação acirrada de canais de comunicação autorizados e ao conteúdo que neles trafegam.

As obstruções de rede, como o firewall, podem tornar o mapeamente de uma rede extremamente difícil. E isso não vai se tornar mais fácil, pois sufocar as sondagens casuais é, freqüentemente, o objetivo principal de se instalar esses dispositivos. Apesar disso, 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 mecanismos 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. Pense com a mente de uma pessoa que quer atacá-lo, e aplique técnicas desta seção contra a sua rede. Lance um scan FTP bounce, um scan idle, um ataque de fragmentação ou tente "tunelar" (criar um túnel) através de um de seus próprios proxies.

Além de restringir a atividade de rede, as empresas estão monitorando o tráfego cada vez mais, 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. Muitos desses produtos foram recentemente metamorfoseados em sistemas de prevenção de intrusão (IPS) que bloqueiam o tráfego considerado malicioso de forma ativa. Infelizmente, para administradores de rede e vendedores de IDS, detectar confiavelmente as más intenções através da análise de dados de pacotes é um problema difícil. Atacantes com paciência, habilidade e a ajuda de certas opções do Nmap podem normalmente passar por um IDS sem serem detectados. Enquanto isso, os administradores devem lidar com um alto número de resultados do tipo falso-positivo, onde atividades inocentes são diagnosticadas erroneamente e recebem alertas ou são bloqueadas.

De vez em quando, as pessoas sugerem que o Nmap não deveria oferecer opções que permitam evitar as regras de firewalls ou passar desapercebidos por IDSs. Elas argumentam que essas características são tão sujeitas à má-utilização por atacantes quanto são utilizadas por administradores para aumentar a segurança. O problema com esta lógica é que esses métodos ainda assim seriam utilizados pelos atacantes, que encontrariam outras ferramentas ou então acrescentariam essa funcionalidade no Nmap. Enquanto isso, os administradores achariam muito mais difícil executar suas tarefas. Instalar apenas servidores FTP modernos e corrigidos é uma defesa muito melhor do que tentar evitar a distribuição de ferramentas que implementem o ataque FTP bounce.

Não existe uma carta mágica (ou opção do Nmap) para detectar e subverter firewalls e sistemas IDS. É necessário habilidade e experiência. Um tutorial está além do escopo deste guia de referência, que apenas lista as opções relevantes e descreve suas funções.

-f (fragmenta os pacotes); --mtu (usando a MTU especificada)

A opção -f faz com que o scan solicitado (incluindo scans usando ping) utilize pequenos pacotes IP fragmentados. A idéia 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. Tenha cuidado com isto! Alguns programas tem problemas para lidar com estes pequenos pacotes. O sniffer da velha-guarda chamado Sniffit sofria uma falha de segmentação assim que recebia o primeiro fragmento. Especifique esta opção uma vez e o Nmap dividirá os pacotes em 8 bytes ou menos após o cabeçalho IP. Portanto, um cabeçalho TCP de 20 bytes seria dividido em 3 pacotes. Dois com oito bytes do cabeçalho TCP e um com os quatro restantes. É claro que cada fragmento também tem um cabeçalho IP. Especifique -f novamente para usar 16 bytes por fragmento (reduzindo o número de fragmentos). Ou então, você pode especificar o seu próprio tamanho de quebra com a opção --mtu. Não especifique também o -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 firewalls que enfilerem 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 isso porque os fragmentos podem seguir por rotas diferentes na rede. Alguns sistemas de origem desfragmentam pacotes de saída no kernel. O Linux e o módulo de reastreamento de conexão do iptables é um exemplo desse tipo. Faça um scan enquanto executa um sniffer como o Ethereal para ter a certeza de que pacotes enviados estão fragmentados. Se o SO do seu host estiver causando problemas, tente a opção --send-eth para passar por cima da camada IP e enviar frames ethernet em estado bruto.

-D <chamariz1 [,chamariz2][,ME],...> (Disfarça um scan usando chamarizes)

Faz com que um scan com chamarizes seja executado, o que parece ao host remoto que, o(s) host(s) que você especificou como chamarizes também estejam escaneando a rede-alvo. Com isso, o IDS poderá reportar 5 a 10 scans de portas de endereços IP únicos, mas não saberá qual IP estava realmente escaneando e qual era um chamariz inocente. Embora isso possa ser desvendado através de rastreamento de caminho de roteador, descarte de respostas (response-dropping) e outros mecanismos ativos, normalmente é uma técnica eficaz para esconder o seu endereço IP.

Separe cada host-chamariz com vírgulas, e você pode opcionalmente usar ME como um dos chamarizes para representar a posição do seu endereço IP real. Se você colocar ME na 6a. posição ou acima, alguns detectores de scan de portas comuns (como o excelente scanlogd da Solar Designer) pouco provavelmente irão mostrar o seu endereço IP. Se você não utilizar o ME, o nmap irá colocá-lo em uma posição aleatória.

Observe que os hosts que você utilizar como chamarizes devem estar ativos ou você poderá, acidentamente, inundar com SYN os seus alvos. Também será bastante fácil determinar qual é o host que está escaneando se houver apenas um host realmente ativo na rede. Você pode preferir usar endereços IP ao invés de nomes (de forma que as redes chamarizes não vejam você em seus logs dos servidores de nomes).

Chamarizes são utilizados tanto no scan com ping inicial (usando ICMP, SYN, ACK ou qualquer outro), como também durante a fase real de escaneamento de portas. Chamarizes também são usados durante a detecção de SO remoto (-O). Chamarizes não funcionam com a detecção de versão ou com o scan TCP connect.

Vale a pena observar que usar chamarizes demais pode deixar seu scan lento e potencialmente até torná-lo menos preciso. Outra coisa, alguns provedores de internet (ISP) irão filtrar os seus pacotes disfarçados, mas muitos não restringem pacotes IP disfarçados.

-S <Endereço_IP> (Disfarça o endereço de origem)

Em algumas circunstâncias, o Nmap pode não conseguir determinar o seu endereço de origem (o Nmap irá dizer se for esse o caso). Nesta situação, use o -S com o endereço IP da interface que você deseja utilizar para enviar os pacotes.

Outro uso possível para esta flag é para disfarçar o scan e fazer com que os alvos achem que alguma outra pessoa está escaneando-as. Imagine uma empresa que está constantemente sofrendo scan de portas de um concorrente! A opção -e normalmente seria requerida para este tipo de uso e -P0 seria recomendável.

-e <interface> (Usa a interface especificada)

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.

--source-port <númerodaporta>; -g <númerodaporta> (Disfarça o número de porta de origem)

Um erro de configuração surpreendentemente comum é confiar no tráfego com base apenas no número da porta de origem. É fácil entender como isso acontece. Um administrador configura um firewall novinho em folha, só 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. O FTP é outro exemplo comum. Em tranferências FTP ativas, o servidor remoto tenta estabelecer uma conexão de volta com o cliente para poder transferir o arquivo solicitado.

Soluções seguras para esses problemas existem, freqüentemente na forma de proxies no nível da aplicação ou módulos de firewall para análise de protocolo. Infelizmente também há soluções mais fáceis e inseguras. Observando que as respostas DNS chegam pela porta 53 e o FTP ativo pela porta 20, muitos administradores caem na armadilha de apenas permitir tráfego vindo dessas portas. Eles normalmente assumem que nenhum atacante irá notar e explorar essas brechas no firewall. Em outros casos, os administradores consideram isso uma medida provisória de curto prazo até que eles possam implementar uma solução mais segura. Então, eles normalmente se esquecem de fazer as atualizações de segurança.

Administradores de rede sobrecarregados não são os únicos a caírem nessa armadilha. Diversos produtos foram empacotados com essas regras inseguras. Mesmo a Microsoft é culpada. Os filtros IPsec que vieram com o Windows 2000 e com o Windows XP contém uma regra implícita que permite todo o tráfego TCP ou UDP da porta 88 (Kerberos). Em outro caso bastante conhecido, versões do firewall pessoal Zone Alarm, até a versão 2.1.25, permitiam qualquer pacote UDP entrante com a porta de origem 53 (DNS) ou 67 (DHCP).

O Nmap oferece as opções -g e --source-port (elas são 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 para que certos testes de detecção de SO funcionem direito, e as requisições DNS ignoram a flag --source-port porque o Nmap confia nas bibliotecas de sistema para lidar com isso. A maioria dos scans TCP, incluindo o scan SYN, suportam a opção completamente, assim como o scan UDP.

--data-length <número> (Acrescenta dados aleatórios nos pacotes enviados)

Normalmente o Nmap envia pacotes minimalistas contendo apenas o cabeçalho. Dessa forma os pacotes TCP têm normalmente 40 bytes e os echo requests ICMP tem só 28. 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 SO (-O) não são afetados, pois a precisão exige consistência das sondagens, mas a maioria dos pacotes de ping e scan de portas funcionam assim. Isso atrasa um pouco as coisas, mas pode tornar um scan ligeiramente menos chamativo.

--ttl <valor> (Establece o valor do campo time-to-live)

Estabelece que o campo tempo-de-vida (time-to-live) dos pacotes enviados terá o valor informado.
--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 e recompile. Uma solução alternativa é gerar uma lista de endereços IP-alvos com um scan de lista (-sL -n -oN <nomedoarquivo>), embaralhar a lista com um script Perl e então fornecer a lista completa para o Nmap com -iL.

--spoof-mac <endereço mac, prefixo, ou nome do fabricante> (Disfarça o endereço MAC)

Solicita ao Nmap que utilize o endereço MAC informado para todos os frames ethernet em estado bruto (raw) 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 (com os pares opcionalmente separados por dois pontos), 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. Se o argumento não for um 0 ou uma string hexa, o Nmap irá procurar no nmap-mac-prefixes para encontrar o nome de um fabricante contendo a string informada (não é sensível a maiúsculas ou minúsculas). Se encontrar, o Nmap usa o OUI (prefixo de 3 bytes) do fabricante e preenche os 3 bytes restantes aleatoriamente. Exemplos de argumentos --spoof-mac válidos são Apple, 0, 01:02:03:04:05:06, deadbeefcafe, 0020F2 e Cisco.

--badsum (Send packets with bogus TCP/UDP checksums)

Solicita ao Nmap que utilize uma soma de verificação (checksum) TCP ou UDP inválida para os pacotes enviados aos hosts. Uma vez que virtualmente todos as pilhas (stack) 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. Para mais detalhes desta técnica, veja http://www.phrack.org/phrack/60/p60-0x0c.txt

Saída (Output)

Qualquer ferramenta de segurança só é útil se a saída que ela gera também o for. Testes e algoritmos complexos são de pouco valor se não forem apresentados de uma forma organizada e compreensível. Dado o número de formas que o Nmap é utilizado pelas pessoas e por outros softwares, nenhum formato irá agradar a todos. Então o Nmap oferece diversos formatos, incluindo o modo interativo para humanos lerem diretamente e o XML para fácil interpretação por um software.

Além de oferecer diversos formatos de saída, o Nmap fornece opções para controlar a verbosidade da saída, bem como das mensagens de depuração. Os tipos de saída podem ser enviados para a saída padrão (standard output) 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 (interactive output), e é enviada para a saída padrão (stdout). Há também a saída normal (normal output), que é 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, ao invés de interativamente.

A saída XML é um dos tipos de saída mais importantes pois permite a conversão para HTML, é facilmente analisada por programas como a interface gráfica do Nmap, ou pode ser importada em banco de dados.

Os dois tipos restantes de saída são a simples saída para o grep (grepable output) que inclui a maioria das informações de um host-alvo em uma única linha e a s4íd4 sCRiPt KiDDi3 (sCRiPt KiDDi3 0utPUt) para usuários que se consideram 1r4d0z (|<-r4d).

Embora a saída interativa seja a padrão e não tenha associada nenhuma opção de linha de comando, as outras quatro opções de formato utilizam a mesma sintaxe. Elas recebem um argumento, que é o nome do arquivo onde os resultados devem ser armazenados. Formatos múltiplos podem ser especificados, mas cada formato só pode ser especificado uma vez. Por exemplo, você pode querer armazenar a saída normal para seu uso enquanto grava a saída XML do mesmo scan para análise utilizando programas. Você pode fazer isso com as opções -oX myscan.xml -oN myscan.nmap. Embora este capítulo use nomes simples como myscan.xml por uma questão de brevidade, nomes mais descritivos normalmente são recomendados. Os nomes escolhidos são uma questão de preferência pessoal, embora eu use nomes longos que incorporam a data do scan e uma palavra ou duas que descrevam o scan, colocados em um diretório com o nome da empresa que eu estou escaneando.

Mesmo que essas opções gravem os resultados em arquivos, o Nmap ainda assim mostra a saída interativa na stdout como de costume. Por exemplo, o comando nmap -oX myscan.xml target grava em XML no myscan.xml e enche a saída padrão com os mesmos resultados interativos que teria mostrado se a opção -oX não tivesse sido especificada. Você pode mudar isso passando um caracter hífen como argumento de um dos tipos de formato. Isso faz com que o Nmap desative a saída interativa e apenas grave os resultados no formato que você especificou para a saída padrão. Dessa forma, o comando nmap -oX - target irá enviar apenas a saída XML para a stdout. Erros sérios ainda podem ser mostrados na saída padrão de erros, stderr.

Ao contrário de alguns argumentos do Nmap, o espaço em branco entre a flag da opção (como a -oX) e o nome do arquivo ou hífen é obrigatório. Se você omitir as flags e informar argumentos como -oG- ou -oXscan.xml, uma característica de compatibilidade retroativa do Nmap irá causar a criação de arquivos de saída do tipo normal format chamados G- e Xscan.xml respectivamente.

O Nmap também oferece opções para controlar a verbosidade do scan e para acrescentar informações nos arquivos de saída, ao invés de sobrepor. Todas essas opções estão descritas abaixo.

Formatos de Saída do Nmap

-oN <especificaçãodearquivo> (Saída normal)

Solicita que a saída normal (normal output) seja direcionada para o arquivo informado. Conforme discutido acima, é um pouco diferente da saída interativa (interactive output).

-oX <especificaçãodearquivo> (Saída em XML)

Solicita que a saída em XML (XML output) seja direcionada para o arquivo informado. O Nmap inclui uma definição do tipo de documento (document type definition, DTD) que permite que os analisadores (parsers) XML validem a saída em XML do Nmap. Embora seja primeiramente voltada para ser usada por programas, também pode ajudar os humanos a interpretar a saída em XML do Nmap. A DTD define os elementos válidos do formato, e geralmente enumera os atributos e valores que eles podem receber. A última versão está sempre disponível em http://insecure.org/nmap/data/nmap.dtd.

O XML oferece um formato estável que é facilmente interpretado por software. Interpretadores (parsers) XML gratuitos estão disponível para as principais linguagens de computador, incluindo C/C++, Perl, Python e Java. As pessoas até já escreveram extensões para a maioria dessas linguagens para manipular a saída e a execução especificamente do Nmap. Exemplos são o Nmap::Scanner e o Nmap::Parser em Perl CPAN. Em quase todos os casos em que uma aplicação não-trivial faz interface com o Nmap, o XML é o formato preferido.

A saída XML faz referência à uma folha de estilo que pode ser usada para formatar os resultados em HTML. A forma mais fácil de se utilizar isso é simplesmente carregar a saída XML em um navegador web como o Firefox ou o IE. Por padrão, isso só irá funcionar na máquina onde você rodou o Nmap (ou em uma máquina similarmente configurada) devido ao caminho (path) do sistema de arquivos (filesystem) gravado de forma inalterável do nmap.xsl. Utilize a opção --webxml ou --stylesheet para criar arquivos XML portáveis que podem ser interpretados como um HTML em qualquer máquina conectada à web.

-oS <especificaçãodearquivo> (S4íd4 ScRipT KIdd|3)

A saída script kiddie é como a saída interativa, com a diferença de ser pós-processada para atender melhor aos "hackers de elite" (l33t HaXXorZ) que antigamente rejeitavam o Nmap devido ao uso consistente de maiúsculas e minúsculas e a grafia correta. Pessoas sem senso de humor devem observar que esta opção serve para se fazer graça dos script kiddies antes de me xingar por estar, supostamente, “ajudando-os”.

-oG <especificaçãodearquivo> (Saída para o grep)

Este formato de saída é mencionado por último porque está depreciado. O formato de saída XML é muito mais poderoso e é bastante adequado para usuário 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 feito por mim. O XML é extensível para suportar novas características do Nmap conforme elas forem lançadas, por outro lado, sempre tenho que omitir essas novas características da saída para o grep por falta de onde colocá-las.

Apesar disso, a saída para o grep é bastante popular. 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. Em mesmo uso-a para testes rápidos feitos na linha de comando. Descobrir todos os hosts com a porta ssh aberta ou que estão rodando o Solaris requer apenas um simples grep para identificá-los, concatenado via pipe a um comando awk ou cut para mostrar os campos desejados.

A saída para o grep consiste de comentários (linhas começadas com o símbolo #) e linhas-alvo. Uma linha-alvo inclui uma combinação de 16 campos rotulados, separados por tab e seguidos por dois-pontos. Os campos são Host, Portas (Ports),Protocolos (Protocols), Estado Ignorado (Ignored State), SO (OS), Índice de Seqüência (Seq Index), IPID e Estado (Status).

O campo mais importante é, normalmente, Portas (Ports), que fornece detalhes de cada porta interessante. É uma lista com a relação de portas, separada por vírgula. Cada porta representa uma porta interessante, e tem o formato de sete sub-campos separados por barra (/). Esses sub-campos são: Número da Porta (Port number), Estado (State), Protocolo (Protocol), Proprietário (Owner), Serviço (Service), informação sobre o SunRPC (SunRPC info) e informação sobre a Versão (Version info).

Assim como na saída XML, esta página man não permite que se documente o formato todo. Uma visão mais detalhada sobre o formato de saída para o grep do Nmap está disponível em http://www.unspecific.com/nmap-oG-output.

-oA <nome-base> (Saída para todos os formato)

Para facilitar, você pode especificar -oA <nome-base> 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, como ~/nmaplogs/foocorp/ no UNIX ou c:\hacking\sco no Windows.

Opções de Verbosidade e depuração (debugging)

-v (Aumenta o nível de verbosidade)

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 fornecidas quando o Nmap acha que um scan irá demorar mais do que alguns minutos. Use duas vezes para uma verbosidade ainda maior. Usar mais do que duas vezes não surte nenhum efeito.

A maioria das alterações afetam apenas a saída interativa, e algumas também afetam a saída normal e script kiddie. Os outros tipos de saída foram feitos para serem processados por máquinas, então o Nmap pode dar informações bastante detalhadas por padrão nesse formatos sem cansarem o usuário humano. Entretanto, existem algumas mudanças nos outros modos onde o tamanho da saída pode ser reduzido substancialmente pela omissão de alguns detalhes. Por exemplo, uma linha de comentário, na saída para o grep, que fornece uma lista de todas as portas escaneadas só é mostrada no modo verboso porque ela pode ser bem longa.

-d [nível] (Aumenta ou estabelece o nível de depuração)

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 (-v), a depuração é habilitada com uma flag na linha de comando (-d) 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 -d. Por exemplo, -d9 estabelece o nível nove. Esse é efetivamente o nível mais alto e irá produzir milhares de linhas, a menos que você execute um scan muito simples com poucas portas e alvos.

A saída da depuração é útil quando há a suspeita de um bug no Nmap, ou se você simplesmente está confuso com o que o Nmap está fazendo e por quê. Como esta opção é, na maioria das vezes, destinada a desenvolvedores, a linhas de depuração nem sempre são auto-explicativas. Você pode obter algo como: Timeout vals: srtt: -1 rttvar: -1 to: 1000000 delta 14987 ==> srtt: 14987 rttvar: 14987 to: 100000. Se você não entender uma linha, suas únicas opções serão ignorá-la, procurar no código-fonte ou pedir ajuda na lista de discussão de desenvolvimento (nmap-dev). Algumas linhas são auto-explicativas, mas as mensagens ficam cada vez mais obscuras conforme o nível de depuração é aumentado.

--packet-trace (Rastreia pacotes e dados enviados e recebidos)

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 usuário entenderem exatamente o que o Nmap está fazendo por baixo dos panos. Para evitar mostrar milhares de linhas, você pode querer especificar um número limitado de portas a escanear, como -p20-30. Se tudo o que lhe interessa for saber o que se passa no subsistema de detecção de versão, use o --version-trace.

--iflist (Lista as interfaces e rotas)

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 (como, por exemplo, no caso do Nmap tratar uma conexão PPP como se fosse uma Ethernet).

--log-errors (Registrar os erros/avisos em um arquivo de sáida em modo normal)

Avisos e erros mostrados pelo Nmap normalmente aparecem apenas na tela (saída interativa), 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. É útil quando você não está vendo a saída interativa ou está tentando depurar um problema. As mensagens continuarão a aparecer no modo interativo. Isto não irá funcionar para a maioria dos erros ligados à argumento inválidos na linha de comando, ocorre que o Nmap pode ainda não ter inicializado seus arquivos de saída ainda. Somado a isso, algumas mensagens de erro/aviso do Nmap utilizam um sistema diferente que ainda não suporta esta opção. Uma alternativa ao uso desta opção é redirecionar a saída interativa (incluindo o fluxo de erros padrão) para um arquivo. Embora a maioria dos shells Unix tornem essa uma alternativa fácil, pode ser difícil fazer o mesmo no Windows.

Opções diversas (miscellaneous) de saída

--append-output (Acrescenta no arquivo de saída, ao invés de sobrepor)

Quando você especifica um nome de arquivo na flag de formato de saída, como -oX ou -oN, esse arquivo é sobreposto por padrão. Se você preferir manter o conteúdo existente do arquivo e acrescentar os novos resultados, especifique a opção --append-output. Todos os arquivos de saída especificados na execução do Nmap terão os resultados acrescidos ao invés de sobrepostos. Isso não funciona bem com os dados de scan para XML (-oX) pois o arquivo resultante não será adequadamente interpretado até que você conserte manualmente.

--resume <nomedoarquivo> (Retoma um scan abortado)

Algumas execuções extensas do Nmap podem levar muito tempo -- na ordem de dias. Tais scans nem sempre rodam até o fim. Podem haver restrições que impeçam que o Nmap seja executado durante o horário de expediente, a rede pode cair, a máquina onde o Nmap está rodando pode sofrer um reboot planejado ou não, ou o Nmap pode simplesmente travar. O administrador que está rodando o Nmap poderia cancelá-lo por qualquer outra razão, bastando teclar ctrl-C. Reiniciar um scan inteiro do começo pode ser indesejável. Felizmente, se forem mantidas logs normal (-oN) ou para o grep (-oG), o usuário pode pedir que o Nmap continue o escaneamento do alvo que estava verificando quando a execução foi interrompida. Simplesmente especifique a opção --resume e informe o arquivo da 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. Basta chamar o Nmap com nmap --resume <nomedoarquivodelog>. O Nmap irá acrescentar os novos resultados ao arquivo de dados especificado na execução anterior. Essa retomada de execução não suporta o formato de saída XML porque combinar as duas execuções em um arquivo XML válido seria difícil.

--stylesheet <caminho ou URL> (Informa a folha de estilo XSL usada para transformar a saída XML)

O Nmap vem com uma folha de estilo (stylesheet) chamada nmap.xsl para visualizar ou traduzir a saída XML em HTML. A saída XML inclui uma diretiva xml-stylesheet que mostra para o nmap.xml onde ele foi inicialmente instalado pelo Nmap (ou para o diretório corrente no Windows). Simplesmente carregue a saída XML do Nmap em um navegador moderno e ele deve conseguir achar o nmap.xsl no sistema de arquivos e utilizá-lo para interpretar os resultados. Se você deseja utilizar uma folha de estilo diferente, especifique-a como um argumento para --stylesheet. Você deve informar o caminho completo ou a URL. Uma chamada comum é --stylesheet http://insecure.org/nmap/data/nmap.xsl. Isso diz ao navegador para carregar a versão mais atual da folha de estilo da Insecure.Org. A opção --webxml faz a mesma coisa com menos teclas e menor memorização. Carregar o XSL da Insecure.org torna mais fácil de se ver os resultados em uma máquina que não tenha o Nmap instalado (e, conseqüentemente o nmap.xsl). Então, a URL é normalmente mais útil, mas a localização nmap.xsl em um filesystem local é usada por padrão por questões de privacidade.

--webxml (Carrega a folha de estilo da Insecure.Org)

Esta opção conveniente é apenas um apelido para --stylesheet http://insecure.org/nmap/data/nmap.xsl.

--no_stylesheet (Omite do XML a declaração da folha de estilo XSL)

Especifique esta opção para evitar que o Nmap associe qualquer folha de estilo XSL à saída XML. A diretiva xml-stylesheet é omitida

Opções Diversas (Miscelânea)

Esta seção descreve algumas opções importantes (e não-tão-importantes) que realmente não couberam em nenhum outro lugar.

-6 (Habilita o escaneamento IPv6)

Desde 2002, o Nmap oferece suporte a IPv6 na maioria de suas opções mais populares. Em particular, o scan com ping (apenas TCP), o scan com connect e a detecção de versão, todo suportam IPv6. A sintaxe de comando é a mesma de sempre, exceto que você irá também adicionar a opção -6. É claro que você deve usar a sintaxe IPv6 se especificar um endereço no lugar de um nome de host. Um endereço pode se parecer com 3ffe:7501:4819:2000:210:f3ff:fe03:14d0, portanto os nomes de host são recomendados. A saída é a mesma de sempre, com o endereço IPv6 na linha "portas interessantes" sendo a única dica visível de se tratar realmente de IPv6.

Muito embora o IPv6 não ter, exatamente, se alastrado pelo mundo, seu uso se torna mais significativo em alguns países (normalmente asiáticos) 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. Se o seu provedor (ISP) (como a maioria) não aloca endereços IPv6 para você, alguns intermediários, que fazem o túnel gratuitamente, estão amplamente disponíveis e funcionam bem com o Nmap. Um dos melhores é disponibilizado pela BT Exact em https://tb.ipv6.btexact.com/. Também tenho utilizado um, fornecido pela Hurricane Electric em http://ipv6tb.he.net/. Túneis 6para4 são outra abordagem gratuita e popular.

-A (Opções agressivas de scan)

Esta opção habilita opções adicionais avançadas e agressivas. Ainda não decidi exatamente qual das duas é a certa. Atualmente ela habilita a Detecção de SO (-O) e o escaneamento de versão (-sV). Mais características poderão ser adicionadas no futuro. A questão é habilitar um conjunto completo de opções de escaneamento sem que as pessoas tenham que se lembrar de um grupo grande de flags. Esta opção apenas habilita as funções e não as opções de temporização (como a -T4) ou opções de verbosidade (-v) que você pode também querer.

--datadir <nomedodiretório> (Especifica a localização dos arquivos de dados do scan)

O Nmap obtém alguns dados especiais, em tempo de execução, em arquivos chamados nmap-service-probes, nmap-services, nmap-protocols, nmap-rpc, nmap-mac-prefixes e nmap-os-fingerprints. O Nmap primeiramente busca esses arquivos em um diretório especificado na opção --datadir (se houver). Qualque arquivo que não seja encontrado lá é procurado no diretório especificado pela

variável de ambiente NMAPDIR. A seguir vem o ~/.nmap para se achar os UIDs reais e efetivos (apenas em sistemas POSIX) ou a localização do executável do Nmap (apenas Win32) e, então, a localização definida na compilação, que pode ser /usr/local/share/nmap ou /usr/share/nmap . Como último recurso, o Nmap irá procurar no diretório corrente.

--send-eth (Use a transmissão pela ethernet em estado bruto)

Solicita ao Nmap para que envie pacotes na ethernet (data link) em estado bruto (raw) ao invés de usar a camada de nível mais alto IP (rede). Por padrão, o Nmap escolhe o que for melhor para a plataforma onde está rodando. Soquetes (sockets) em estado bruto (camada IP) são normalmente mais eficientes em máquinas UNIX, enquanto que os frames ethernet são necessários nas operações do Windows, uma vez que a Microsoft desabilitou o suporte a soquetes em estado bruto. O Nmap ainda usa pacotes IP em estado bruto no UNIX, independentemente desta opção, quando não há outra alternativa (como no caso de conexões não-ethernet).

--send-ip (Envia no nível do IP em estado bruto)

Pede ao Nmap que envie os pacotes pelos soquetes IP em estado bruto ao invés de enviar pelo nível mais baixo dos frames ethernet. É o complemento da opção --send-eth discutida anteriormente.

--privileged (Assume que o usuário é altamente privilegiado)

Informa ao Nmap para simplesmente assumir que ele tem privilégio suficiente para executar transmissões de soquetes em estado bruto, farejar (sniff) 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. --privileged é útil com as possibilidades oferecidas pelo kernel do Linux, e sistemas similares, que pode ser configurado para permitir que usuários não-privilegiados executem scans de pacotes em estado bruto. Assegure-se de informar esta flag de opção antes de outras flags de opção que requeiram privilégios (scan SYN, detecção de OS, etc.). A variável NMAP_PRIVILEGED pode ser configurada como uma alternativa equivalente de --privileged.

--release-memory (Release memory before quitting)

Esta opção é útil apenas para depuração de vazamentos de memória (memory-leak). 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.

--interactive (Inicial em modo interativo)

Inicia o Nmap em modo interativo, que oferece um prompt interativo do Nmap, permitindo o início de múltiplos scans (tanto síncronos quanto em background). Isto é útil para pessoas que escaneiam a partir de sistemas multi-usuários e que normalmente querem testar a segurança sem deixar todo mundo saber exatamente quais sistemas eles estão escaneando Use --interactive para ativar este modo e então tecle h para uma ajuda (help). Esta opção é raramente utilizada porque um shell adequado é mais familiar e tem mais opções. Esta opção inclui um operador exclamação (!) para a execução de comandos de shell, o que é uma das muitas razões de não se instalar o Nmap com setuid root.

-V; --version (Mostra o número da versão)

Mostra o número da versão do Nmap e sai.

-h; --help (Mostra a página do sumário de ajuda)

Mostra uma pequena tela com as flags de comandos mais comuns. Executar o nmap sem nenhum argumento faz a mesma coisa.

Interação em Tempo de Execução

Durante a execução do Nmap, todas as teclas pressionadas são capturadas. Isso permite que você interaja com o programa sem abortá-lo ou reiniciá-lo. Algumas teclas especiais irão mudar as opções, enquanto outras irão mostrar uma mensagem de estado dando informações sobre o scan. A convenção é que letras minúsculas aumentam a quantidade de informação e letras maiúsculas diminuem. Você também pode pressionar '?' para obter ajuda.

v / V
Aumenta / Diminui a quantidade de informações (Verbosity)

d / D
Aumenta / Diminui o Nível de Depuração (Debugging Level)

p / P
Habilita / Desabilita o Rastreamento de Pacotes (Packet Tracing)

?
Mostra uma tela de ajuda da interação em tempo de execução

Qualquer outra letra

Mostra uma mensagem de estado como esta:
Stats: 0:00:08 elapsed; 111 hosts completed (5 up), 5 undergoing Service Scan
Service scan Timing: About 28.00% done; ETC: 16:18 (0:00:15 remaining)

Exemplos

Aqui estão alguns exemplos de utilização do Nmap, desde o simple e rotineiro, até o um pouco mais complexo e esotérico. Alguns endereços IP reais e nomes de domínio foram utilizados para tornar as coisas mais concretas. Nesses lugares você deve substituir os endereços/nomes pelos da sua própria rede. Embora eu não ache que o escaneamento de portas de outras redes seja, ou deva ser considerado, ilegal alguns administradores de rede não apreciam o escaneamento não-solicitado de suas redes e podem reclamar. Obter a permissão antecipadamente é a melhor opção.

Para fins de teste, você tem permissão para escanear o host scanme.nmap.org. Esta permissão inclui apenas o escaneamento via Nmap e não tentativas de explorar vulnerabilidades ou ataques de negação de serviço (denial of service). Para preservar a banda, por favor não inicie mais do que uma dúzia de scans contra o host por dia. Se esse serviço de alvo livre para escaneamento for abusado, será derrubado e o Nmap irá reportar Failed to resolve given hostname/IP: scanme.nmap.org. Essas permissões também se aplicam aos hosts scanme2.nmap.org, scanme3.nmap.org, e assim por diante, embora esses hosts ainda não existam.

nmap -v scanme.nmap.org

Esta opção escaneia todas as portas TCP reservadas na máquina scanme.nmap.org . A opção -v habilita o modo verboso (verbose).

nmap -sS -O scanme.nmap.org/24

Inicia um scan SYN camuflado contra cada máquina que estiver ativa das 255 possíveis da rede “classe C” onde o Scanme reside. Ele também tenta determinar qual o sistema operacional que está rodando em cada host ativo. Isto requer privilégio de root por causa do scan SYN e da detecção de SO.

nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

Inicia uma enumeração de hosts e um scan TCP na primeira metade de cada uma das 255 sub-redes de 8 bits possíveis na classe B do espaço de endereçamento 198.116. Também testa se os sistemas estão executando sshd, DNS, pop3d, imapd ou a porta 4564. Para cada uma destas portas encontradas abertas, a detecção de versão é usada para determinar qual aplicação está executando.

nmap -v -iR 100000 -P0 -p 80

Pede ao Nmap para escolher 100.000 hosts de forma aleatória e escaneá-los procurando por servidores web (porta 80). A enumeração de hosts é desabilitada com -P0 uma vez que enviar primeiramente um par de sondagens para determinar se um hosts está ativo é um desperdício quando se está sondando uma porta em cada host alvo.

nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20

Este exemplo escaneia 4096 endereços IP buscando por servidores web (sem usar o ping) e grava a saída nos formatos XML e compatível com o programa grep.

Autor

Fyodor <fyodor@insecure.org> (http://insecure.org)

Centenas de pessoas fizeram contribuições valiosas para o Nmap ao longo dos anos. Isso está detalhado no arquivo CHANGELOG que é distribuído com o Nmap e também está disponível em http://insecure.org/nmap/changelog.html.