**Scanner de Portas - Nmap** - [www.nmap.org](http://www.nmap.org/)
Artigo Básico de [www.invasao.com.br](http://www.invasao.com.br/)

Os escaneadores de hosts são ferramentas úteis a administradores de rede e consultores de segurança ou utilitários usados por hackers para invasão? Esse dilema segue os usuários dessas ferramentas cada vez mais populares e fáceis de usar. Seja qual for seu objetivo este artigo tentará elucidar a forma de utilização e os principais recursos de um dos mais conhecidos escaneadores existentes, o Nmap.

**O Nmap**

O Nmap é um escaneador de hosts que usa recursos avançados para verificar o estado do seu alvo. A ferramenta é gratuita e encontrada nas versões Linux, Windows, Mac OS, Solaris, FreeBSD e OpenBSD. As versões para Windows e Linux contam com uma interface gráfica que facilitam a vida dos usuários. Aqui **analisaremos a versão para Linux**, porém o funcionamento varia pouco em outros sistemas operacionais.

**Obtendo e instalando**

O download pode ser feito no site oficial, em [http://www.insecure.org](http://www.insecure.org/). A instalação pode ser feita a partir do pacote RPM disponivel no site. Como root(superusuário), instale com o seguinte comando:

rpm -vhi http://download.insecure.org/nmap/dist/nmap-3.30-1.i386.rpm

Assim o programa será baixado e instalado diretamente do site oficial do Nmap.
Caso você use uma distribuição que não suporte RPM, como Debian ou Slackware, baixe os fontes e compile. Para isso baixe o arquivo com o comando:

wget http://download.insecure.org/nmap/dist/nmap-3.30.tar.bz2

Agora descompacte com o comando:

bzip2 -cd nmap-3.30.tar.bz2 | tar xvf -

Entre no diretório criado com o comando:

cd nmap-3.30

Agora compile e instale:

./configure
make
make install

Utilização do Nmap:

Apesar de existirem os front-ends gráficos disponíveis, os comando passados em modo texto permitem uma enorme flexibilidade e, ao contrário do que possa parecer, o uso não é difícil. A sintaxe do comando sempre será:

nmap [ <Scan Type> ...] [ <Options> ] { <target specification> }

Onde o (target) é o endereço IP do alvo (host) ou rede que se deseja escanear. Caso exista uma forma de resolver nomes, como um DNS configurado, você pode usar o nome do host ao invés do IP. Com a opção -p podemos especificar portas ou faixas (ranges) de portas para análise. Os parâmetros são ajustados de acordo com o que se deseja obter, os principais são:

-sT - Com esse parâmetro é feito um escaneamento através de tentativas de conexão TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS;
-sS – Assim, a tentativa será com pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão. Essa técnica dificulta um pouco a detecção;
-sP - Com essa opção o escaneamento será feito através de pacotes ICMP echo request. Verifica apenas se o host está ativo;
-sU - Envia pacotes UDP com 0 byte para determinar o estado dessas portas;
-sO - É usado para tentar determinar os protocolos suportados pelo host;
-O - Com esse parâmetro é feito uma tentativa de determinar o sistema operacional através de uma técnica conhecida como Active FingerPrint.

**Bom, esses são os principais parâmetros, com eles podemos realizar os mais variados testes.

Vamos partir para a prática.

Primeiro testo com pacotes SYN, nas portas de 1 a 100, no meu próprio roteador:**

nmap -sS 192.168.0.1 -p 1-100

Recebi uma resposta assim:



O que me mostra que tenho um serviço SSH(usado para acesso remoto) aberto na porta 22.
Você pode escanear um endereço de rede para determinar serviços ativos em mais de um host, basta para isso informar o endereço da rede, como no exemplo:

**nmap -sS 192.168.0.0/24 -p 1-150**



Os resultados são mostrados para todos os hosts da rede separadamente. Essa técnica é interessante pra identificar falhas de segurança em toda sua rede interna.

Agora tentaremos um alvo fora da minha rede interna. Tentaremos o IP 168.143.xx.48, omitiremos obviamente parte do endereço analisado.

**nmap -sT 168.143.xx.48**



Note que não especificamos um intervalo de portas, assim todas as portas serão escaneadas e nosso teste poderá demorar bastante dependendo do nosso link. Aqui tentamos uma análise por tentativas de conexão TCP(opção -sT) ao invés de apenas envio de solicitações de conexão(opção -sS). É fácil observar que existem muitos serviços ativos e suas respectivas portas.

Por último tentaremos identificar o sistema operacional de um alvo em nossa rede local, para isso usaremos o parâmetro -O, assim:

**nmap -O 192.168.0.66**


Em nosso teste o sistema operacional foi identificado perfeitamente, como pode ser visto na figura acima.

Como se defender

Utilitários como o Nmap estão em constante atualização, cada vez mais sutis eles passam muitas vezes desapercebidos no firewalls e IDSs. O que pode diminuir os riscos é a configuração de firewalls com regras bem definidas, diminuição dos serviços ativos no gateway deixando apenas aqueles indispensáveis ao seu funcionamento e análise constante de seus arquivos de log. Um bom sistema de detecção de intrusos, como o SNORT, é indicado também.

O Nmap pode e deve ser usado para averiguação do estado do seu host, principalmente se tratar de um servidor. Use, constantemente, para monitorar o estado das portas e se elas pertencem a algum serviço legitimo ou não.

Portas abertas podem significar trojans ou outras forma de programas de exploração de ataques instalados, por isso use também o programa **chkrootkit** para identificar mais facilmente essa tentativa de ataque. O **chkrootkit** pode ser encontrado no endereço <http://www.chkrootkit.org>.

**Conclusão**

O Nmap pode ser considerado uma ferramenta Hacker / Cracker, ou um excelente utilitário para consultores de segurança e administradores de rede, o fato é que ele realiza de forma extremamente eficiente o que se propõe.

**De site ::LINUXIT::**

[**http://www.linuxit.com.br**](http://www.linuxit.com.br/)

**Modos de varredura suportados pelo Nmap**

» TCP **Connect: -sT --** Varredura de Portas connect () TCP completa. Esse é o padrão e a única varredura disponível quando o usuário sendo executado não for root.

» Varredura furtiva TCP SYN: -sS -- Só envia um único pacote SYN - o primeiro pacote do handshake TCP de três vias. Se receber um SYN &#124; ACK, então, saberá qual máquina está escutando nessa porta. Não encerra o handshake TCP, o que significa que geralmente não é registrado como um connect () real seria. Refere-se freqüentemente a essa conexão com uma varredura semi-aberta.

» Varredura baseada na RFC 793 …

» Varredura FIN: -sF -- Varredura FIN. Um pacote FIN básico é enviado. Se um RST for recebido, a porta está fechada. Se nada for recebido, a porta deve estar aberta.
Como o Windows não segue a especificação IP, ele não é detectado por esse método.

» Varredura Xmas Tree: -sX -- Varredura Xmas Tree. Da mesma forma que a varredura FIN, ela usa um pacote com conjuntos de flags FIN, URG e PUSH.

» Varredura Null: -sN -- Modo de Varredura Null. Semelhante a FIN, porém usando um pacote sem qualquer flag.

» Varredura Microsoft e a RFC 793 ... (Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

» Varredura UDP: -sU -- O Nmap enviará um pacote UDP sem bytes para cada porta da máquina de destino. Se uma porta ICMP que não puder ser acessada for retornada, quer dizer que estará fechada. Essa varredura tende a ser incomodamente lenta devido a um sugestão da RFC 1812 que limita a taxa de mensagens de erro do ICMP. Se o Nmap fosse executado da maneira mais rápida possível, perderia o retorno em potencial da maioria dos pacotes ICMP. Em vez disso, o Nmap detectará a taxa que o host está usando e diminuirá a velocidade de sua varredura de acordo com essa informação.

» Varredura ACK: -sA -- Varredura ACK. Esta varredura é útil para mapear conjuntos de regras que estão ativas nos firewalls e determina se o firewall é um firewall com estados ou um filtro de bloqueio de pacotes SYN simples. O Nmap envia um pacote ACK, que normalmente indica o recebimento bem-sucedido de um pacote, para cada uma das portas. Já que não há uma conexão estabelecida, um pacote RST deve retorna se a porta não estiver sendo filtrada pelo firewall.

» Varredura TCP Window: Usa o tamanho da janela do protocolo TCP -sW -- Varredura de janela. Esta varredura, semelhante a ACK, usa o tamanho da janela TCP para determinar se as portas estão abertas, e se estão sendo filtradas ou não. Felizmente, o Linux não é vulnerável a essa varredura, embora seu firewall possa ser.

» Varredura FIN/ACK: -sM (Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

» Varredura RPC: -sR (Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

» Varredura BOUNCE: (Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

» Varredura baseada no cabeçalho do Protocolo IP: -sO -- Varreduras do protocolo IP. Determina quais protocolos IP são suportados da máquina de destino. O Nmap envia pacotes IP brutos para cada protocolo.
Se um protocolo ICMP que não pode ser acessado for retornado, significará que é suportado. Alguns sistemas operacionais e firewalls não enviam os pacotes ICMP e parecerá que todos os protocolos são suportados.

» Varreduras ICMP e Discovery: -sP (Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

» Formas Furtivas Varreduras: Permite uma varredura de forma discreta, desviando a atenção do administrador e seus aparatos de segurança.

(Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

» Varreduras Temporizadas:

(Ver ref. Sandro Melo, Exploração de Vulnerabilidade em Redes TCP/IP, Caps. 4 e 5)

-------------------------------------------------------------------------------------------

» Fingerprint de OS com o Nmap: -O -- Detecção de sistema operacional.

Relembrando o Formato de comandos Nmap:

nmap [ <Scan Type> ...] [ <Options> ] { <target specification> }

# nmap -O ip.ip.ip.ip

# nmap -O -p80 ip.ip.ip.ip O invasor tenta ser mais discreto usando somente 1 porta.

# nmap -O -p21 -osscan\_guess ip.ip.ip.ip (-osscan\_guess = modo de verificação máxima)
--------------------------------------------------------------------------------------------------

**Algumas** **Opções de Configuração do Nmap normalmente usadas:**

**Ver todas as opções de configurações em** [**http://nmap.org/book/man-briefoptions.html**](http://nmap.org/book/man-briefoptions.html)

**»** -n – Nunca fazer a resolução DNS.

» -PO -- Normalmente o Nmap executará o ping no host antes de pesquisá-lo. Se você souber que uma \*máquina está sendo executada ou suspeitar que está bloqueando pacotes de ping ICMP, use esse flag para forçar a varredura de qualquer forma.

» -A – Leitura de banners

» -I -- Varredura de identificação reversa. O Nmap se conectará à porta (com um connect() completo - as varreduras furtivas não funcionarão com esse modo) e, se conectado, consultará o servidor identificado no destino para determinar o nome de usuário que está escutando. Assim você poderá saber se o root ou outro usuário esta com a porta ligada/ativa.

» -f -- Pacotes de varredura em fragmentos. Um pacote TCP pode ser fragmentado em elementos menores, que são reagrupados no host. Muito filtros e firewalls de pacotes não os reagrupam e, portanto, podem permitir que passem por onde não deveriam, assim a varredura pode passar pelo software de detecção de intrusos.

» -v -- Modo de informações detalhadas.

» -vv -- Modo de informações muito detalhadas. Se você quiser as entranhas dos pacotes do Nmap, será desse modo.

» -D -- Hosts-isca. Envia pacotes de varredura como se também fossem de nomes de host listados. Já que seu host se encontra em uma lista de host fictícios, você pode ser capaz de se ocultar no meio da balbúrdia. Se os pacotes IP falsificados forem bloqueados entre host de varredura do nmap e o destino, eles nunca chegarão lá.

» -T -- Política de intervalos de tempo. Já que alguns detectores de varredura procuram uma certa quantidade de pacotes inadequados em um intervalo de tempo definido, usar varreduras mais lentas pode torná-los inócuos. As opções existentes vão de Paranoid, que envia um pacote a cada 5 minutos, á Insane, que só aguarda 0,3 segundo para o tempo de espera da sondagem e pode perder informações devido à sua velocidade.