Autor: ryuuu
Contato: ryuuu__@hotmail.com

Nmap – Diferenças entre estados de porta (Parte 1)

"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." (http://nmap.org).

Existem muitos portscans eficientes e que possivelmente poderiam substituir o nmap, mas eles não reconhecem um estado de porta como o nmap, eles simplesmente distinguem uma porta entre aberta (open) ou fechada (closed). Já o nmap refinou sua pesquisa por portas, definindo-as em seis estados:

- Aberta (open): Atribui-se o estado open, para as portas que estão ativamente aceitando conexões TCP ou pacotes UDP nesta porta. Saiba que uma porta em estado open, é um convite para um ataque.

- Fechada (closed): Uma porta em estado closed, está acessível, porém não possui nenhuma aplicação "escutando" nela. Portas closed são úteis para mostrar o endereço IP de determinado host.

- Filtrada (filtered): O Nmap não consegue determinar se uma porta está aberta pelo fato da mesma estar com uma filtragem de pacotes que impede a sondagem de alcançar essa porta. Essa filtragem pode ser um dispositivo firewall dedicado, regras de roteador, ou um software de firewall baseado em host. Em alguns casos essas portas respondem com mensagens de erro ICMP do tipo 3 código 13 (destino inalcançável: comunicação proibida administrativamente), mas os filtros que simplesmente descartam pacotes sem mesmo responder são bem mais comuns. Sendo assim, o nmap acredita que os pacotes podem ter sido descartados devido ao congestionamento da rede, forçando-o a tentar várias vezes. Isso reduz a velocidade do scan drasticamente.

- Não-filtrada (unfiltered): Unfiltered significa que a porta está acessível, porém o nmap não consegue determinar se a porta está aberta ou fechada. Apenas

o scan ACK, que é usado para mapear conjuntos de regras de firewall, classifica portas nesse estado. Usar outros métodos de escaneamento, como Scan Window, Scan Syn, Scan FIN, podem ajudar a determinar se a porta está aberta.

- Open | Filtered: Esse estado é usado pelo nmap quando o mesmo não consegue determinar se a porta está aberta ou filtrada. Isso acontece para tipos de scan onde as portas abertas não dão nenhuma resposta. Essa falta de pacotes também pode significar que um filtro de pacotes descartou a sondagem ou qualquer tipo de resposta que ela provocou. Os scans UDP, IP Protocol, FIN, Null e Xmas classificam portas nesse estado.

- Closed | Filtered: Esse estado é usado pelo nmap quando o mesmo não consegue determinar se aporta está fechada ou filtrada. É apenas usado para o scan IP ID Idle Scan.

Nmap – Técnicas de escaneamento de portas

O Nmap possui várias técnicas de escaneamento de portas, abaixo segue uma lista explicando cada técnica. *Lembrando: As técnicas de scan citadas abaixo devem ser utilizadas como usuário root, em Linux, e Administrador, em Windows.

- -sS (TCP SYN): É uma técnica muito popular e muito eficiente. Essa técnica pode facilmente determinar se uma porta está open, closed ou filtered, e geralmente é chamada de half-open scanning, pois não abre uma conexão TCP completa (não completa o handshake) e funciona da seguinte maneira.

  - Para uma porta aberta:

  Source >>>>>>>>>>>>>>>> TCP SYN >>>>>>>>>>>>>>> Destination

  Source <<<<<<<<<<<<<< TCP SYN/ACK <<<<<<<<<<<< Destination

  - *Para uma porta fechada*:

  Source >>>>>>>>>>>>>>>> TCP SYN >>>>>>>>>>>>>>> Destination

Source <<<<<<<<<<<<<<< TCP RST <<<<<<<<<<<<< Destination

- *Para uma porta filtrada*:

Source >>>>>>>>>>>>>>> TCP SYN >>>>>>>>>>>>>> Destination

Source <..... Destination

OU

Quando recebe um erro ICMP Port Unreachable (porta inalcancável) (tipo 3, código 1, 2, 3, 9, 10 ou 13).

- *-sT (TCP Connect)*: Esse scan é igual ao scan SYN, porém estabelece uma conexão com a máquina e a porta do host (3-way handshake) enviando uma chamada de sistema connect(). Essa chamada é a mesma utilizada por browsers, clientes P2P, e a maioria das outras aplicações de rede. É a parte da interface de programação conhecida como API de Sockets de Berkeley. O nmap utiliza esta API para obter informações do estado de cada tentativa de conexão. Esse scan funciona da seguinte maneira.

  - *Quando estabelece uma conexão (porta aberta)*:

  Source >>>>>>>>>>>>>>> TCP SYN >>>>>>>>>>>>>> Destination

  Source <<<<<<<<<<<<< TCP SYN/ACK <<<<<<<<<<< Destination

  Source >>>>>>>>>>>>>>> TCP ACK >>>>>>>>>>>>>> Destination

  - *Para definir portas como, fechada ou filtrada*:

  Mesmo esquema da técnica -sS.

- *-sU (UDP Scan)*: É utilizado para escanear portas UDP. É normalmente mais lento e mais difícil que o TCP. Vários serviços utilizam essas portas, tais como DNS (53), SNMP (161/162) e DHCP (67/68), e podem estar vulneráveis.

Ele pode ser combinado com algum scan de TCP, como por exemplo o SYN Scan, averiguando ambos protocolos.

Esse scan envia um cabeçalho UDP vazio (sem dados) para cada porta. E funciona da seguinte maneira:

- *Para portas abertas*: Como resposta, vem outro pacote UDP.
- *Para portas fechadas*: Como resposta, vem um erro ICMP Port Unreachable tipo 3, código 3.
- *Para portas filtradas*: Como resposta, vem um erro ICMP Port Unreachable tipo 3, códigos 1, 2, 9, 10 ou 13.
- *Para portas abertas* | *filtradas*: Como resposta, não vem nada, significando que a porta poderia estar aberta, porém filtros de pacotes estão impedindo a comunicação.

Scans de versões (-sV) podem ser utilizados ajudar a para diferenciar as portas verdadeiramente abertas das que estão filtradas.

- *-sN; -sF; -sX (TCP Null, FIN e Xmas)*: Esses três tipos de scan são os mesmos em termos de comportamento, exceto pela flag marcadas no pacote de sondagem. A vantagem desses scans é que eles podem sondar hosts através de firewall não-orientado à conexão e roteadores que filtram pacotes. Outra vantagem é que eles são menos perceptíveis que o Scan SYN. Mas não se engane, IDS's bem configurados podem detectar esses tipos de scan.

  Esse scan funciona da seguinte maneira:

  - *Para portas abertas* | *filtradas*:

  Source >>>>>>>>> TCP Null, FIN ou Xmas >>>>>>>>>> Destination

  Source <..... Destination

  - *Para portas fechadas*:

  Source >>>>>>>>> TCP Null, FIN ou Xmas >>>>>>>>>> Destination

  Source <<<<<<<<<<<<<<< TCP RST <<<<<<<<<<<<< Destination

  - *Para portas filtradas*: ICMP Port Unreachable tipo 3, código 1, 2, 3, 9, 10 ou 13.

- *-sA (TCP ACK)*: Esse scan nunca definirá uma porta como aberta ou aberta | filtrada. Ele é usado para descobrir regras de firewall, determinando se eles são orientados a conexão ou não e quais portas estão filtradas.

Se um sistema é não-filtrado, as portas abertas e fechadas respondem com um pacote RST. Então:

- *Para portas unfiltered*:

Source >>>>>>>>>>>>>>>> TCP ACK >>>>>>>>>>>>>> Destination

Source <<<<<<<<<<<<<<<< TCP RST <<<<<<<<<<<<<< Destination

- *Para portas filtradas*:

Source >>>>>>>>>>>>>>>> TCP ACK >>>>>>>>>>>>>> Destination

Source <..... Destination

OU

Quando a resposta for uma mensagem de erro ICMP Port Unreachable tipo 3, código 1, 2, 3, 9, 10 ou 13.

- *-sW (TCP Window)*: Trabalha igual o Scan ACK, mas com um detalhe, ele analisa o campo TCP Window to pacote RST de resposta. Em alguns SO's esse valor pode ser positivo, para portas abertas, ou zero, para portas fechadas. Mas como isso não é uma regra, então esse scan não é muito confiável. Alguns sistemas que não suportam isso irão normalmente devolver zero, sendo assim, todas portas “estarão” fechadas.

- *-sM (TCP Maimon)*: Tem esse nome devido ao seu descobridor, Uriel Maimon. Ele descreveu essa técnica na Phrack Magazine, edição 49 (Novembro de 1996). Essa técnica é a mesma que os scans Null, FIN e Xmas, exceto que a sondagem é FIN/ACK. Segundo 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 Personalizado)*: Técnica de scan para usuários que não querem se limitar às técnicas de scan que o nmap oferece.

Para escolher qual flag usar, você pode usar valores numéricos, como 9 para PSH e FIN, mas usar seus nomes é mais fácil. E para isso, apenas digite, sem espaços, os nomes desejados. Por exemplo, --scanflags URGACKPSHRSTSYNFIN marca tudo. A ordem em que essas marcas são especificadas é irrelevante.

Além de especificar a flag usada, você pode combinar a flag que você escolheu, com as respostas base dos scans do Nmap. Por exemplo: O scan SYN considera nenhuma resposta como porta filtrada, por outro lado o scan FIN considera como aberta | filtrada. Então ele usará as flags que você especificar, porém usará esses outros scans como resposta base. Não escolher nenhuma, significa que será utilizado o Scan SYN.

- *-sI (Scan Idle)*: Esse tipo de scan, na verdade, faz um spoofing de algum IP que você queira. É bom para descobrir relações de confiança entre hosts, ou seja, se determinado host possui relações de confiança com o outro (“spoofado” por você), então mais detalhes serão mostrados.

  As máquinas que são “spoofadas”, são chamadas de zumbis.

Se você quiser, pode usar : (dois pontos) seguido de algum número de porta, ao IP do host zumbi, para sondar por outra porta. Caso nada for especificado, ele usa a porta padrão para pings tcp (porta 80).

- *-sO (Scan de protocolo IP)*: Esse scan é utilizado para descobrir quais protocolos são suportados pelo host alvo (TCP, ICMP, IGMP, etc.). Pode ser usado a opção -p para selecionar os números de protocolo a escanear.

O Scan de protocolo funciona de forma similar ao scan de 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 protocolo. As três exceções são TCP, UDP e ICMP, porque alguns SO's não os enviarão caso não os tenham e também porque o nmap tem as funções para criá-los. Ao invés de verificar as mensagens de erro ICMP Port Unreachable, o Nmap observa as mensagens ICMP Protocol

Unreachable. Se for recebido qualquer mensagem de qualquer protocolo, então este é marcado como aberto. Um erro ICMP Protocol Unreachable tipo 3, código 2, é marcado como fechado. Outros erros de ICMP Protocol Unreachable tipo 3, código 1, 3, 9, 10 ou 13, são marcados como filtrados (embora eles provem, ao mesmo tempo, que o ICMP está aberto). Se não vier nenhuma resposta, o protocolo é marcado como aberto | filtrado.

- *-b (Scan de FTP bounce)*: Esse tipo de scan é usado em servidores vulneráveis a Proxy FTP. Isso permite que um usuário conecte-se a um servidor FTP, e então solicite que arquivos sejam enviados a um segundo servidor. Tal característica é sujeita a abusos em diversos níveis. Um dos abusos seria fazer um servidor escanear as portas de outro. Para isso, basta solicitar ao servidor para enviar um arquivo para cada porta interessante do alvo. Então a partir da mensagem de erro, é determinado se a porta está aberta ou fechada. Esta é uma boa forma de passar por 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 argumento desse tipo de scan é:

  <nomeusuario>:<senha>@<servidor>:<porta>.

Assim como em URL normal, você pode omitir <nomedousuario>:<senha>, neste caso as credenciais de logins são anonimas (usuário: anonymous, senha: -wwwuser@) são usados. O número da porta (e os dois pontos) podem ser omitidos, e então é usado a porta padrão FTP (21).

Referências:

1. http://nmap.org/man/pt_BR/man-port-scanning-basics.html
2. http://nmap.org/man/pt_BR/man-port-scanning-techniques.html