Autor: ryuuu
Contato: ryuuu__@hotmail.com

Nmap - Detecção de SO (Parte 2)

Para realizar uma detecção de SO remota, o nmap utiliza a identificação da pilha do TCP/IP (stack fingerprinting). Ele envia uma série de pacotes TCP e UDP ao host e examina praticamente todos os bits das respostas. “Após executar dezenas de testes como a amostragem TCP ISN (Initial Sequence Number), suporte e ordenamento das opções do TCP, amostragem IP ID 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.” (http://nmap.org/), mostrando o nome do fabricante, SO base, geração do SO, e tipo de dispositivo.

Quando a opção verbose (-v) é usada juntamente com a opção -O, é mostrado a geração de sequência IP ID. A maioria das máquinas é classificada como “incremental”, isso significa que elas incrementam o campo ID do cabeçalho IP para cada pacote que envia. Isso torna-as vulneráveis a ataques avançados de levantamento e forjamento de informações.

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

- -O: Habilita a detecção de SO. Também pode ser usado a opção -A para habilitar tanto a detecção de SO quanto a detecção de versão.
- --osscan-limit: Limita a detecção do SO a alvos promissores, ou seja, o nmap não irá nem tentar detectar o SO do alvo se o host não corresponder 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: Se o nmap não conseguir fazer a detecção exata do SO, ele oferece possibilidades aproximadas. Mas a correspondência tem que ser muito próxima para o nmap fazer isso como padrão. O nmap ainda assim

irá dizer quando uma correspondência imperfeita é mostrada e o nível de confiança (porcentagem) de cada suposição.

*Existe outro meio de descobrir o SO, e chama-se captura de banner. É um método muito simples, para fazê-lo, tente se conectar em alguma porta usando telnet e espere pela resposta. Geralmente nessa resposta vem o tipo e a versão do SO instalada.

Entendendo o fingerprinting

Fingerprint, traduzindo ao pé da letra, seria “impressão digital”, como nós humanos, possuímos nossa impressão digital, que é única para cada um, os SO's também possuem. Essa técnica é extremamente poderosa e muito confiável. O Nmap utiliza a pilha TCP/IP do SO para descobrir qual SO o alvo está usando, uma vez que cada desenvolvedor faz diferentes implementações dessas pilhas (por isso é possível descobrir). *Obs: Essa técnica necessita de pelo menos uma porta aberta.

Há várias maneiras de obter o fingerprint, abaixo segue algumas:

- *Manipulação de fragmentação*: Citado por Thomas Ptacek e Tim Newsham, cada pilha TCP/IP manipulam os fragmentos diferentemente. Por exemplo, quando os fragmentos são remontados, algumas sobrescrevem os dados antigos com os novos, ou vice-versa. Sabendo como os pacotes são remontados, podemos saber qual SO a máquina está usando;

- *Pacote FIN*: Se é enviado um pacote FIN para determinada porta, o correto do SO é não responder, mas alguns SO's respondem com FIN/ACK, como o Windows NT;

- *Padrão TCP de ISN (TCP ISN Sampling)*: Essa técnica identifica o SO a partir do modo como é elaborado o número inicial de sequência. Solaris, IRIX e FreeBSD usam padrão randômico de incrementação, sistemas Windows usam um modelo que está vinculado com o horário do sistema. Sistemas Unix antigos de 64k eram famosos por serem fáceis de burlar.

- *Tamanho da janela inicial do TCP*: Essa técnica trabalha com a informação do tamanho da janela de um pacote. Scanners de fingerprint mais inteligentes são capazes de utilizarem esse valor de um datagrama, pois alguns possuem valores específicos como o AIX, como também existem alguns com valores similares. É o caso da pilha TCP/IP do Windows, que possui o mesmo valor do FreeBSD e OpenBSD.

- *Flag falso (BOGUS Flag)*: Implementado no QUESO, consiste em enviar um datagrama TCP com flag de valor (64 ou 128) no cabeçalho de um pacote TCP de início de conexão (bit SYN ativo). A maior parte dos SO's retornam um pacote RST.

- *Bit não fragmentar*: É verificado se o bit não fragmentar está ligado ou não. Em alguns SO's, é configurado para obter melhor desempenho.

- *Valor ACK*: É verificado o campo ACK do TCP/IP. Em alguns SO's, devolvem o número da sequência enviado, em outros, o [número da sequência + 1].

- *ICMP*: Analisa as mensagens ICMP respondidas pelo host, fazendo de 1 a 4 testes.

    - Dentre as análises das mensagens ICMP respondidas pelo host, abaixo segue algumas delas que podem ser usadas como fingerprint:

        - Campo IP:

            - *Tamanho*: O tamanho do campo IP pode variar entre alguns SO's. Na família BSD, por exemplo, é adicionado 20 bytes nesse campo. Alguns outros diminuem 20 bytes, e alguns apenas repetem o mesmo tamanho.

            - *Checksum (verificação da soma do cabeçalho)*: Alguns SO's, nesse campo, irão calcular erroneamente, enquanto outros irão apenas zerar, e alguns apenas repetem o campo.

- Cabeçalhos IP de pacotes ICMP respondidos:
  - *TTL (Time-To-Live)*: Possuem dois valores, um para consultar mensagens ICMP, outro para responder as consultas. A verificação desses valores podem ajudar na detecção do SO.
  - *TOS (Tipe-Of-Service)*: “O uso do TOS com mensagens ICMP eh diferente entre mensagens de erro ICMP (destination unreachable, source quench, redirect, time exceeded e parameter problem), mensagens de consulta (echo, router solicitation, timestamp, information request, address mask request), e mensagens de respostas (echo reply, router advertisement, timestamp reply, information reply, address mask reply)” (http://www.angelfire.com)

    O RFC 1349 dita algumas regras:

    - Uma mensagem de erro ICMP eh sempre enviada com o valor TOS padrao (0);
    - Uma mensagem de solicitaçao ICMP pode ser enviada com qualquer valor no TOS;
    - Uma mensagem de resposta ICMP eh enviada com o mesmo valor no TOS que foi usado na mensagem de solicitaçao ICMP.

    Alguns SO's ignoram o RFC e apenas repetem a mensagem de resposta ICMP.
- Cabeçalhos ICMP de pacotes ICMP respondidos:
  - *Tamanho das mensagens de erro*: De acordo com o RFC 792, somente 8 octetos (64 bits) do datagrama original são incluídos nas mensagens ICMP de erro. Porém, o RFC 1122, que foi lançado depois, recomenda 576 octetos.

    Alguns SO's seguem o antigo, outros, como o Linux/HPUX 11.x, Solaris e MacOS, adicionam mais octetos.

- *Repetição de mensagens de erro*: Alguns SO's enviam mensagens de ICMP de erro de um jeito, alterando os cabeçalhos IP e alguns dados do protocolo, repetindo a mensagem de erro. Então é possível fazer algumas suposições do SO do host.

- Outros:
  - *Valores de campos diferentes de zero em "ICMP echo request"*: Quando é enviado um pedido de "ICMP echo request", alguns SO's zeram esse campo ICMP, outros apenas repetem o mesmo valor.
  - *Outras mensagens*:
    - ICMP Timestamp request;
    - ICMP Information request;
    - ICMP address mask request.

Algumas pilhas TCP/IP suportam estas mensagens e respondem a algumas dessas consultas.

Os testes/sondas feitas por fingerprint, através do nmap, estão a seguir:

- **Sequence Generation (SEQ, OPS, WIN and T1)**

Para gerar essas quatro respostas, o nmap envia uma série de seis sondas TCP, onde cada uma precisam gastar exatamente 110 ms (milisegundos), dando um total de 550 ms. Esse tempo exato é importante, pois alguns testes (como ISN, IP ID, e TCP Timestamp) dependem do tempo.

Cada sondagem envia um pacote TCP SYN para verificar uma porta aberta no alvo. A sequencia e o reconhecimento são aleatórios (mas o nmap guarda-os para poder diferenciar as respostas). A precisão da detecção necessita de uma sondagem consistente, então não há dados de payload, mesmo se o usuário requerer uma com --data-length.

O valor, desses pacotes, do campo TCP Window e as opções TCP variam. Abaixo segue uma lista com as opções e valores de todos seis pacotes. O valor do campo Window listado não reflete à medição do mesmo. O EOL é a opção End-Of-Option-List, e não é mostrada, por padrão, por maioria dos sniffers.

- **Packet #1**: window scale (10), NOP, MSS (1460), timestamp (TSval: 0xFFFFFFFF; TSecr: 0), SACK permitted. The window field is 1.
- **Packet #2:** MSS (1400), window scale (0), SACK permitted, timestamp (TSval: 0xFFFFFFFF; TSecr: 0), EOL. The window field is 63.
- **Packet #3:** Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), NOP, NOP, window scale (5), NOP, MSS (640). The window field is 4.
- **Packet #4:** SACK permitted, Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), window scale (10), EOL. The window field is 4.
- **Packet #5:** MSS (536), SACK permitted, Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), window scale (10), EOL. The window field is 16.
- **Packet #6:** MSS (265), SACK permitted, Timestamp (TSval: 0xFFFFFFFF; TSecr: 0). The window field is 512.

Esses testes resultam em SEQ, OPS, WIN e T1, onde SEQ é baseado na sequencia da análise dos pacotes sondados. Esses resultados são GCD, SP, ISR, TI, II, TS e SS. O próximo, OPS, contém a opção TCP recebida de cada sondagem (o nome dos testes vão de 01 a 06). O WIN, contém o tamanho do campo Window (nomeado de W1 a W6). E o último, T1, contém vários valores de teste para o pacote #1. Os resultados são testes R, DF, T, TG, W, S, A, F, O, RD e Q. Esses resultados são reportados apenas na primeira sondagem, desde que eles sejam quase sempre os mesmos para cada sondagem.

- **ICMP Echo (IE)**

Esse teste envia dois pacotes ICMP Echo Request para o alvo. O primeiro tem o bit IP DF ligado, o TOS (Type-Of-Service) igual a 0, código igual a nove, número de sequência igual a 295, IP ID e identificador ICMP Request aleatório, e um caracter aleatório repetido cento e vinte vezes no payload. O segundo é similar, exceto que um TOS de quatro (IP_TOS_RELIABILITY) é usado, seu código é zero,

cento e cinquenta bytes de dados é enviado, e o IP ID, Request ID, e a sequencia dos números de um do valor da Query anterior.

O resultados desses dois testes são combinados em uma linha IE contendo os testes R, DFI, T, TG, e CD. O R é apenas verdadeiro (Y) se as duas sondagens deduzirem a resposta. O T e o CD são para a resposta da primeira sondagem, uma vez que são altamente improváveis de diferirem. DFI é um teste personalizado para esses dois casos ICMP especiais.

- **TCP explicit congestion notification (ECN)**

Esse teste é baseado no TCP Stack e melhora a performance da internet permitindo que os roteadores enviem sinais de problemas decongestionamento antes que eles comecem a descartar os pacotes. Isso é documentado na RFC 3168. O Nmap testa isso enviando um pacote SYN contendo as flags de controle de congestionamento ECN CWR e ECE ligados. Para um teste não relatado, o campo urgente, de valor 0xF7F5 é usado mesmo que a flag urgente não for ligada. O número de reconhecimento é zero, número de sequência é aleatório, window size é três, e o bit reservado que antecede o bit CWR é ligado. As opções TCP são: Wscale (10), NOP, MSS (1460), SACK Permitted, NOP, NOP. Essa sondagem é enviada para uma porta aberta.

Se uma resposta é recebida, os testes R, DF, T, TG, W, O, CC e Q são feitos e gravados.

- **TCP (T2-T7)**

Cada um dos testes que vão de T2 até T7, enviam um pacote TCP de sondagem. Com uma exceção, a opção TCP Data, em cada caso é (em hex) 03030A0102040109080AFFFFFFFF000000000402. Esses 20 bytes correspondem a Window Scale (10), NOP, MSS (265), Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), SACK Permitted. A exceção é que T7 usa Window Scale de 15 ao invés de 10. As características que variam de cada sondagem está descrita abaixo:

- **T2** sends a TCP null (no flags set) packet with the IP DF bit set and a window field of 128 to an open port.

- **T3** sends a TCP packet with the SYN, FIN, URG, and PSH flags set and a window field of 256 to an open port. The IP DF bit is not set.
- **T4** sends a TCP ACK packet with IP DF and a window field of 1024 to an open port.
- **T5** sends a TCP SYN packet without IP DF and a window field of 31337 to a closed port.
- **T6** sends a TCP ACK packet with IP DF and a window field of 32768 to a closed port.
- **T7** sends a TCP packet with the FIN, PSH, and URG flags set and a window field of 65535 to a closed port. The IP DF bit is not set.

Para cada caso, uma linha é adicionada ao fingerprint com resultado para os testes R, DF, T, TG, W, S, A, F, O, RD, e Q.

Caso o nmap não consiga determinar o SO, e as condições forem favoráveis (por exemplo: com pelo menos uma porta aberta e uma fechada), o nmap fornecerá uma URL onde você poderá enviar a identificação se souber (com certeza) o SO em execução.

- **UDP (U1)**

Esse teste envia um pacote UDP a uma porta fechada. O caracter 'C' (0x43) é repetido trezentas vezes no campo dados. O valor de IP ID é 0x1042 para SO's que permitem esse valor. Se a porta estiver realmente fechada e não tiver firewall no local, o Nmap espera pela resposta ICMP Port Unreachable. Essa resposta é, depois, submetida ao testes R, DF, T, TG, IPL, UN, RIPL, RID, RIPCK, RUCK e RUD.

Referências:

1. http://nmap.org/man/pt_BR/man-os-detection.html
2. http://nmap.org/book/osdetect-methods.html
3. http://www.angelfire.com/linux/resistenciazine/fingerprinting.txt

4. http://www.linuxsecurity.com.br/revista/LinuxSecurityMagazine-Julho02.pdf