NMAP : Identificar a versão de um serviço

Segurança

Vamos falar sobre a forma como o NMAP pode identificar a versão de um serviço que está operando em uma porta. Primeiramente, vamos analisar o que motiva a saber as versões dos serviços em uma porta. Dessa forma, temos que verificar qual o objetivo da verificação, por exemplo verificar a necessidade de atualizar serviços que estão com vulnerabilidades ou investigar um serviço específico. Assim o NMAP utiliza algumas técnicas de sondagem para obter informações suficientes para indicara probabilidade de existência de um serviço e seu versão.

Além disso, em alguns casos temos serviços que usam as mesmas portas bem conhecidas e isso pode levar a uma identificação do serviço de forma incorreta. Devido a isso, o site do NMAP explica que um serviço como o Checkpoint

Firewall-1 GUI pode usar a mesma porta que o yak Windows chat. Nesse caso específico os dois serviços usam a porta 258 TCP. Apresentaremos mais detalhes teóricos no final do artigo.

O NMAP utiliza a opção **-sV** para fazer a varredura de serviços e versões. Alternativamente, podemos usar o -A que também pode ser usado para identificar a versão de serviços. O comando abaixo é usado para verificar a as versões em um host 192.168.0.2. Podemos verificar os serviços que foram detectados e suas respectivas versões.

nmap –sV 192.168.0.2

```
└─$ nmap -sV 192.168.0.2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-08 14:34 EDT
Nmap scan report for 192.168.0.2
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        ProFTPD 1.3.5rc3
22/tcp  open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet     Linux telnetd
80/tcp  open  http       Apache httpd 2.4.7 ((Ubuntu))
443/tcp open  ssl/https Apache/2.4.7 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
Nmap done: 1 IP address (1 host up) scanned in 21.33 seconds
```

Resultado do nmap -sV

Print do wireshark

```
FTP      118 Response: 220 ProFTPD 1.3.5rc3 Server (Debian) [192.168.0.2]
TCP       66 37958 → 21 [ACK] Seq=1 Ack=53 Win=64256 Len=0 TSval=1764638943 TSecr=20587
TCP       66 37958 → 21 [FIN, ACK] Seq=1 Ack=53 Win=64256 Len=0 TSval=1764638943 TSecr=20587
TCP       66 21 → 37958 [ACK] Seq=53 Ack=2 Win=29056 Len=0 TSval=20588 TSecr=1764638943
TCP       66 21 → 37958 [FIN, ACK] Seq=53 Ack=2 Win=29056 Len=0 TSval=20588 TSecr=1764638943
TCP       66 37958 → 21 [ACK] Seq=2 Ack=54 Win=64256 Len=0 TSval=1764638946 TSecr=20588
SSH      110 Server: Protocol (SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13)
TCP       66 37314 → 22 [ACK] Seq=1 Ack=45 Win=64256 Len=0 TSval=1764638954 TSecr=20589
```

Verificando as sondas do nmap -sV

Opção para incluir todas as portas

–allports : essa opção usada em conjunto com o –sV permite verificar todas as portas do host. Dessa forma, portas normalmente excluídas como a porta 9100 usadas por impressoras serão verificadas. Assim, vale ressaltar que algumas portas, como a 9100, podem fazer com que a impressora imprima páginas devido aos dados que são enviados na varredura do NMAP.

nmap –sV –allports 192.168.0.2

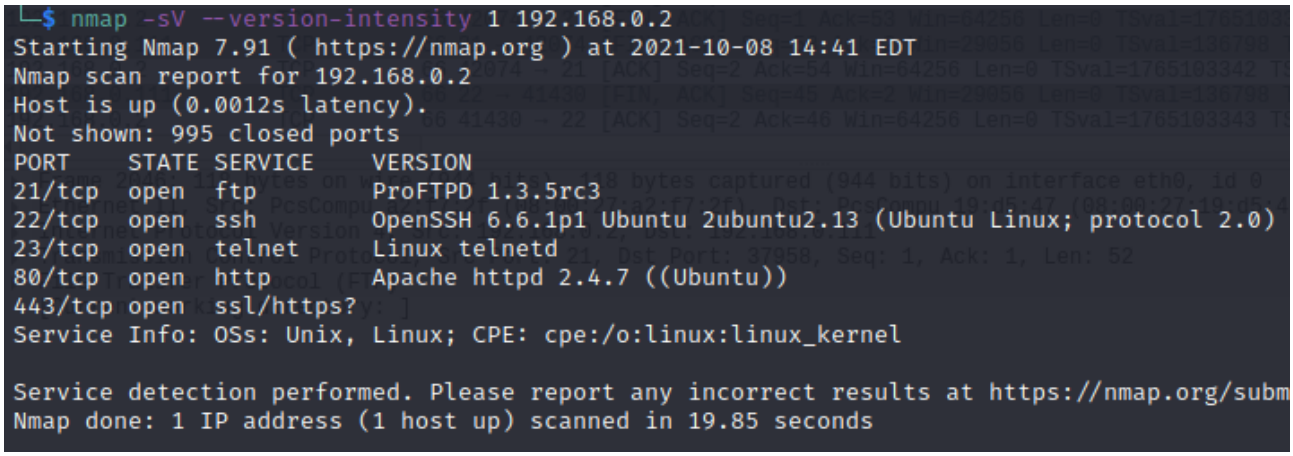
Opção para intensidade na sondagem

–version-intensity 0-9 : utilizando a opção -sV, são enviadas uma serie de sondagens com
o Nmap. È possível aumentar o número de sondagens alterando o valor do **–version-intensity.** Dessa forma, se desejamos que sejam enviados testes de sondagens para serviços mais comuns podemos usar valores baixos no **–version-intensity.**

No entanto, se desejamos utilizar um maior número de testes de sondagem devemos aumentar o valor do **–version-intensity.** Entretanto, vale ressaltar que utilizando valores de **–version-intensity** maiores, a varredura do NMAP vai demorar mais. Além disso, vale lembrar que o valor tem que estar entre 0 e
9. Adicionalmente, o modo default usa o valor 7 de intensidade.

No entanto quando a varredura é direcionada a uma porta específica serão feitos testes adicionais específicos de serviços que operam na porta em questão. Dessa forma, independentemente do grau de intensidade as sondagens dos serviços típicos das portas específicas também serão testadas.

nmap –sV –version-intensity 5 192.168.0.2



Resultado usando intensidade = 1 , Podemos observar que não foi detectado a aplicação na porta 443.

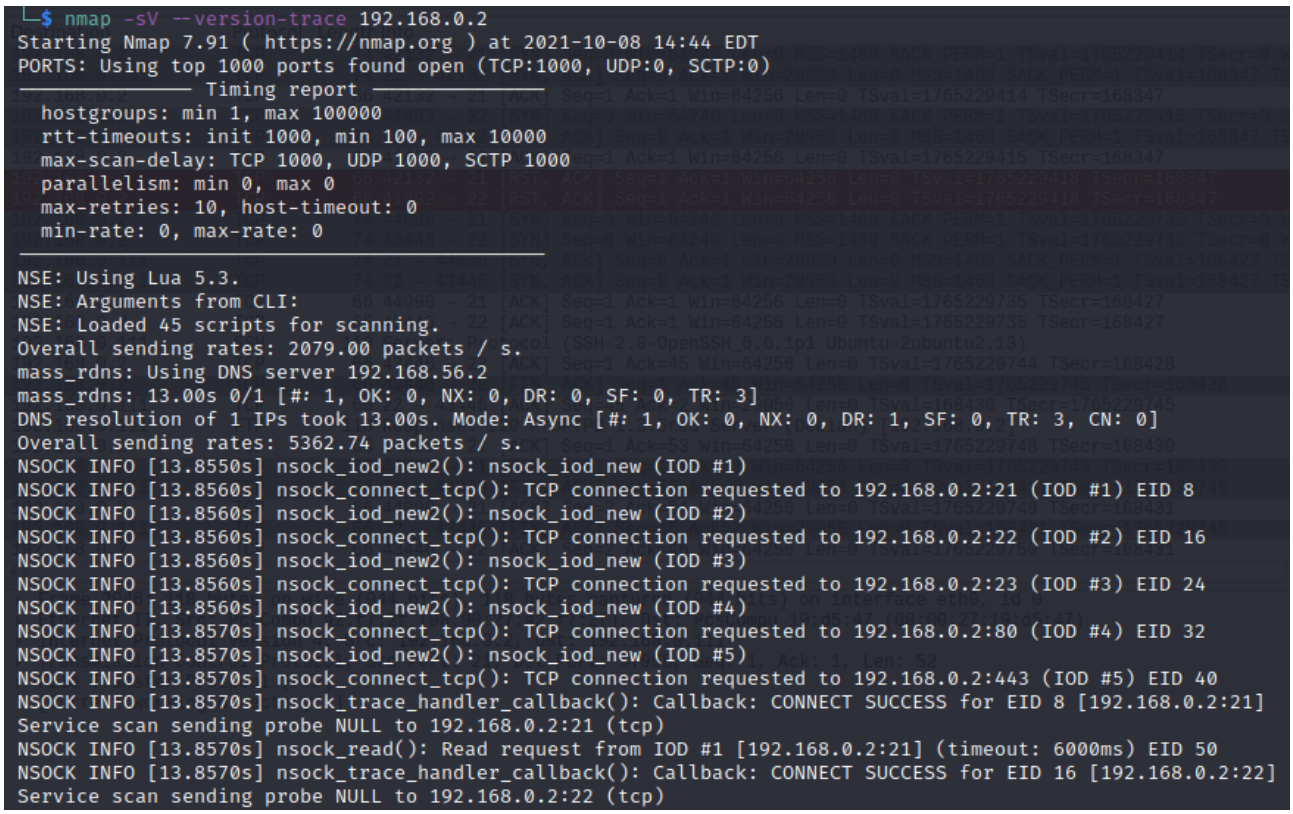
Mais opções de sondagem

–version-light : é o mesmo que usar **–version-intensity 2**. Consequentemente, é

uma forma mais rápida de fazer a verificação, porém com menor probabilidade de identificação.

–version-all : é o mesmo que usar **–version-intensity 9**. Consequentemente, é uma forma mais lenta de fazer a verificação, porém com maior probabilidade de identificação.

–version-trace: apresenta informações adicionais sobre o que a versão de escaneamento está fazendo.



nmap –version-trace

Mais teoria sobre scan de serviços e versões no NMAP

A investigação de tipo de serviço e versão pode revelar mais informações descobertas sobre um serviço são coletadas no campo “info”. Assim, essa informação é exibida na coluna VERSÃO entre parênteses após o nome e a versão. Além disso, este campo pode incluir números de protocolos, como os usados no SSH e módulos como os do servidor Apache.

Além disso, alguns serviços podem informar o nome do host e apresentar uma diferença em relação ao nome provido pelo DNS. Dessa forma, o administrador de rede dever verificar se a informação de hostname apresenta algum risco de exposição de informação não desejada.

O scan baseado em versão e identificação de serviços também pode ser usado para especular o sistema operacional do host. Isso porque, existem serviços que somente operam em um único sistema operacional. Dessa forma, uma vez que o serviço descoberto operar apenas em um sistema operacional o NMAP pode deduzir o sistema operacional do host.

O banco de dados do nmap-service-probes contém sondas para verificar vários serviços e expressões de correspondência usadas para identificar e analisar respostas. Dessa forma, o NMAP tenta verificar qual é o protocolo de serviço , o nome do aplicativo do servidor, o número da versão, nome do

host, tipo de dispositivo do host e o sistema operacional.

Além disso, o nmap-service-probes pode obter a representação Common Platform Enumeration (CPE) das informações coletadas. Assim,
é possivel identificar se um servidor X está operacional para conexões e versões do protocolo usado no SSH. As opções descritas permitem que o NMAP possa Identificar corretamente a versão de um serviço.