Nmap for Pentester: Output Format Scan

December 4, 2020 By Raj Chandel

Nmap which is also known as **Network Mapper** is one of the best open-source and the handiest tool that is widely used for security auditing and network scanning by pentesters. It also provides an additional feature where the results of a network scan can be recorded in various formats.

Table of Contents

Introduction- Scan Output Formats

Pentesters sometimes notice that it becomes troublesome to come up with reports in an explicit format where conducting network scans in giant organizations is extremely tedious. Many organizations make a huge mistake by not using the right set of tools to prepare the report for the output that is derived from the scans.

The Nmap tool has the capability to prepare scan results in various formats which gives the pentester multiple options like generating an HTML page, CSV formats, scripting language etc. So let us explore all the scan output options provided by nmap and look at how useful it can be to any organization depending on their need.

SCAN OUTPUT	
OPTION	DESCRIPTION
-oN	Normal Scan Output
-oX	XML Scan Output
-oG	Grepable Scan Output
-oA	Alias Scan Output

Nmap Scan Report in Normal Format

-oN *<filespec>*

In this format of the scan output, it requests that a normal output is directed to a particular filename. This option can be used to combine with any port or host scanning technique as per the need of the pen tester. The various combinations of the output scans have been demonstrated ahead in the article.

Creating a Normal Nmap report in a simple text format:

```
nmap -oN scan.txt 192.168.1.108
```

```
root@kali:~# nmap -oN scan.txt 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 11:37 EST
Nmap scan report for 192.168.1.108
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@kali:~# cat scan.txt
# Nmap 7.91 scan initiated Thu Nov 19 11:37:33 2020 as: nmap -oN sc
Nmap scan report for 192.168.1.108
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)
```

If a pentester wants to create the scan reports in Normal as well as XML form in a combination.:

```
nmap -oN scan.txt -oX scan.xml 192.168.1.108
```

```
root@kali:~# nmap -oN scan.txt -oX scan.xml 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 11:42 EST
Nmap scan report for 192.168.1.108
Host is up (0.000091s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~# cat scan.txt
# Nmap 7.91 scan initiated Thu Nov 19 11:42:05 2020 as: nmap -oN scan.txt
Nmap scan report for 192.168.1.108
Host is up (0.000091s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)
```

Here you see that the port numbers, the state of the ports and the type of the packet that determined the state of the port or the host.

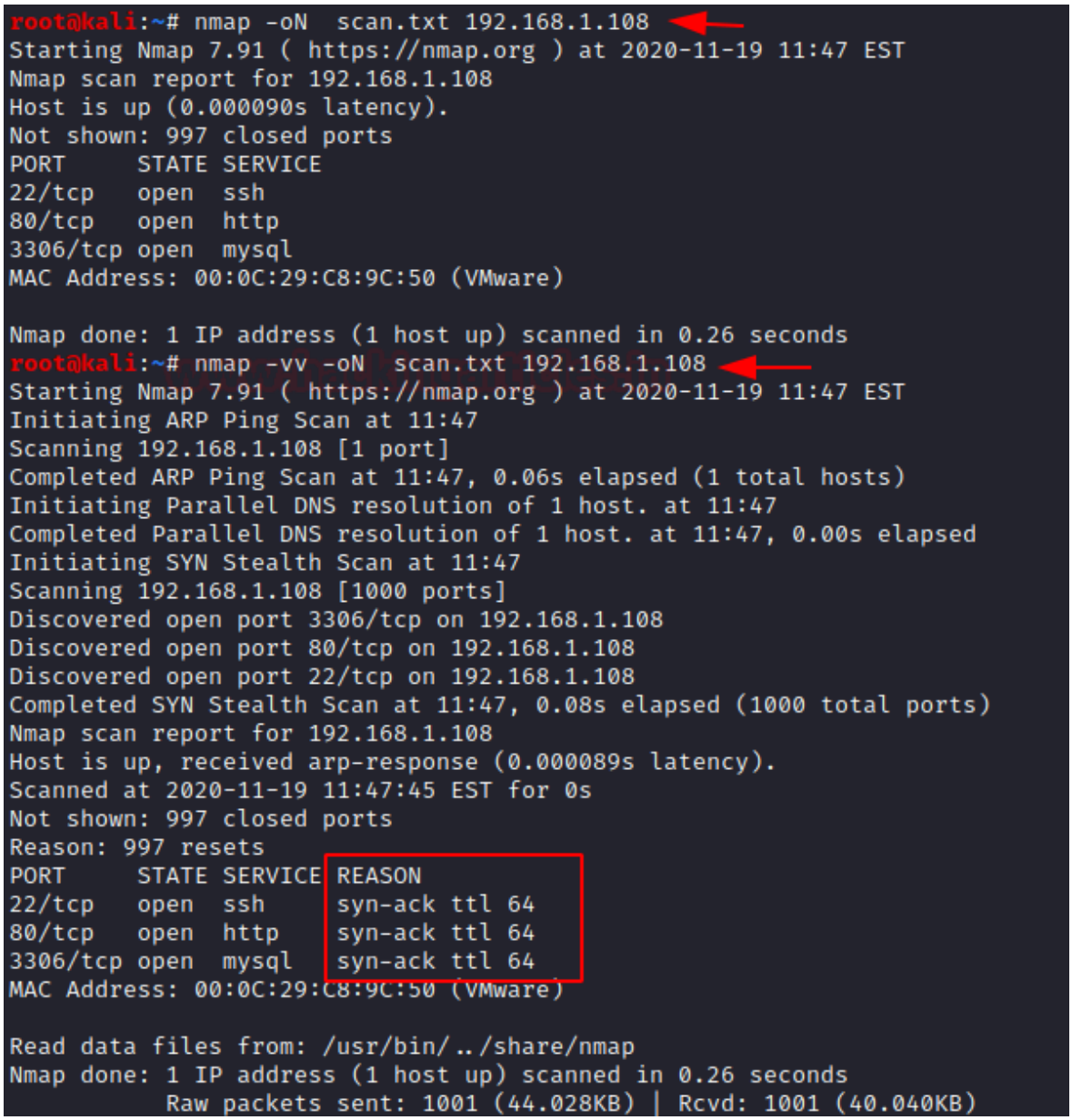
```
<verbose level="0"/>
<debugging level="0"/>
<hosthint><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="192.168.1.108" addrtype="ipv4"/>
<address addr="00:0C:29:C8:9C:50" addrtype="mac" vendor="VMware"/>
<hostnames>
</hostnames>
</hosthint>
<host starttime="1605804125" endtime="1605804125"><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="192.168.1.108" addrtype="ipv4"/>
<address addr="00:0C:29:C8:9C:50" addrtype="mac" vendor="VMware"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="997">
<extrareasons reason="resets" count="997"/>
</extraports>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ssh" meth
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" met
<port protocol="tcp" portid="3306"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="mysql"
</ports>
<times srtt="91" rttvar="9" to="100000"/>
</host>
<runstats><finished time="1605804125" timestr="Thu Nov 19 11:42:05 2020" summary="Nmap done at Thu Nov 19 11:42
>
</runstats>
</nmaprun>
```

Verbosity mode

To increase the level of verbosity for printing more information about the scan . In this scan details like open ports, estimated time of completion, etc are highlighted.

This mode is used twice or more for better verbosity: -vv, or give a verbosity level directly, like -vv, v2, v3.

```
nmap -vv -oN  scan.txt 192.168.1.108
```



Debugging mode

Debugging mode is generally used when the verbose mode doesn't provide enough details about the scan, so it digs deeper into the scanning process. The level of debug can be increased by specifying its number. Here you get details like the flags [resent in the packets, the time-to-live etc.

```
nmap -d2 -oN  scan.txt 192.168.1.108
```

```
root@kali:~# nmap -d2 -oN  scan.txt 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 11:49 EST
Fetchfile found /usr/bin/../share/nmap/nmap-services
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
Fetchfile found /usr/bin/../share/nmap/nmap.xsl
The max # of sockets we are using is: 0
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
```

```
PORT      STATE  SERVICE              REASON
1/tcp     closed tcpmux               reset ttl 64
3/tcp     closed compressnet          reset ttl 64
4/tcp     closed unknown              reset ttl 64
6/tcp     closed unknown              reset ttl 64
7/tcp     closed echo                 reset ttl 64
9/tcp     closed discard              reset ttl 64
13/tcp    closed daytime              reset ttl 64
17/tcp    closed qotd                 reset ttl 64
19/tcp    closed chargen              reset ttl 64
20/tcp    closed ftp-data             reset ttl 64
21/tcp    closed ftp                  reset ttl 64
22/tcp    open   ssh                  syn-ack ttl 64
23/tcp    closed telnet               reset ttl 64
24/tcp    closed priv-mail            reset ttl 64
25/tcp    closed smtp                 reset ttl 64
26/tcp    closed rsftp                reset ttl 64
30/tcp    closed unknown              reset ttl 64
32/tcp    closed unknown              reset ttl 64
33/tcp    closed dsp                  reset ttl 64
37/tcp    closed time                 reset ttl 64
42/tcp    closed nameserver           reset ttl 64
43/tcp    closed whois                reset ttl 64
49/tcp    closed tacacs               reset ttl 64
53/tcp    closed domain               reset ttl 64
70/tcp    closed gopher               reset ttl 64
79/tcp    closed finger               reset ttl 64
80/tcp    open   http                 syn-ack ttl 64
```

Another such command:

```
nmap -dd -oN  scan.txt 192.168.1.108
```

```
root@kali:~# nmap -dd -oN  scan.txt 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 11:51 EST
Fetchfile found /usr/bin/../share/nmap/nmap-services
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
Fetchfile found /usr/bin/../share/nmap/nmap.xsl
The max # of sockets we are using is: 0
-------------- Timing report --------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
-------------------------------------------
Fetchfile found /usr/bin/../share/nmap/nmap-payloads
Initiating ARP Ping Scan at 11:51
Scanning 192.168.1.108 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0×000C29B2 and arp[22:2] = 0×BB
ultrascan_host_probe_update called for machine 192.168.1.108 state UNKNOWN → HOST_UP (t
Fetchfile found /usr/bin/../share/nmap/nmap-mac-prefixes
MAC prefix 080030 is duplicated in /usr/bin/../share/nmap/nmap-mac-prefixes; ignoring du
MAC prefix 0001C8 is duplicated in /usr/bin/../share/nmap/nmap-mac-prefixes; ignoring du
MAC prefix 080030 is duplicated in /usr/bin/../share/nmap/nmap-mac-prefixes; ignoring du
Changing ping technique for 192.168.1.108 to ARP
Changing global ping host to 192.168.1.108.
Completed ARP Ping Scan at 11:51, 0.08s elapsed (1 total hosts)
Overall sending rates: 12.79 packets / s, 537.06 bytes / s.
mass_rdns: Using DNS server 192.168.1.1
NSOCK INFO [0.1610s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1610s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (IO
NSOCK INFO [0.1610s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout: -
Initiating Parallel DNS resolution of 1 host. at 11:51
NSOCK INFO [0.1610s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192.168
NSOCK INFO [0.1610s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8
NSOCK INFO [0.1610s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27
NSOCK INFO [0.3300s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [
NSOCK INFO [0.3300s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout: -
NSOCK INFO [0.3300s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.3300s] nevent_delete(): nevent_delete on event #34 (type READ)
mass_rdns: 0.17s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 11:51, 0.17s elapsed
DNS resolution of 1 IPs took 0.17s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1
Initiating SYN Stealth Scan at 11:51
192.168.1.108 pingprobe type ARP is inappropriate for this scan type; resetting.
Scanning 192.168.1.108 [1000 ports]
Packet capture filter (device eth0): dst host 192.168.1.9 and (icmp or icmp6 or ((tcp or
```

```
Discovered closed port 8080/tcp on 192.168.1.108
Discovered closed port 443/tcp on 192.168.1.108
Discovered closed port 199/tcp on 192.168.1.108
Discovered closed port 139/tcp on 192.168.1.108
Discovered closed port 110/tcp on 192.168.1.108
Discovered closed port 1723/tcp on 192.168.1.108
Discovered closed port 256/tcp on 192.168.1.108
Discovered closed port 25/tcp on 192.168.1.108
Discovered closed port 113/tcp on 192.168.1.108
Discovered closed port 587/tcp on 192.168.1.108
Discovered open port 22/tcp on 192.168.1.108
Discovered closed port 53/tcp on 192.168.1.108
Discovered closed port 993/tcp on 192.168.1.108
Discovered closed port 143/tcp on 192.168.1.108
Discovered closed port 1720/tcp on 192.168.1.108
Discovered closed port 445/tcp on 192.168.1.108
Discovered closed port 3389/tcp on 192.168.1.108
Discovered closed port 5900/tcp on 192.168.1.108
Discovered closed port 135/tcp on 192.168.1.108
Discovered open port 3306/tcp on 192.168.1.108
Discovered open port 80/tcp on 192.168.1.108
Discovered closed port 554/tcp on 192.168.1.108
Discovered closed port 21/tcp on 192.168.1.108
Discovered closed port 8888/tcp on 192.168.1.108
Discovered closed port 23/tcp on 192.168.1.108
Discovered closed port 995/tcp on 192.168.1.108
Discovered closed port 1025/tcp on 192.168.1.108
```

Nmap Scan Report in XML Format

-oX *<filespec>*

It stands for Extensible Markup Language which is a tree-structured file format that is supported by Nmap.

The results from the Nmap scan can be exported into an XML file and can be further used for analysis or another additional task.

When an XML report is generated, it contains information like an executed command, Host and port states, Nmap Scripting Engine output Services, Timestamps, Run statistics and debugging information.

```
nmap -oX scan.xml 192.168.1.108
```

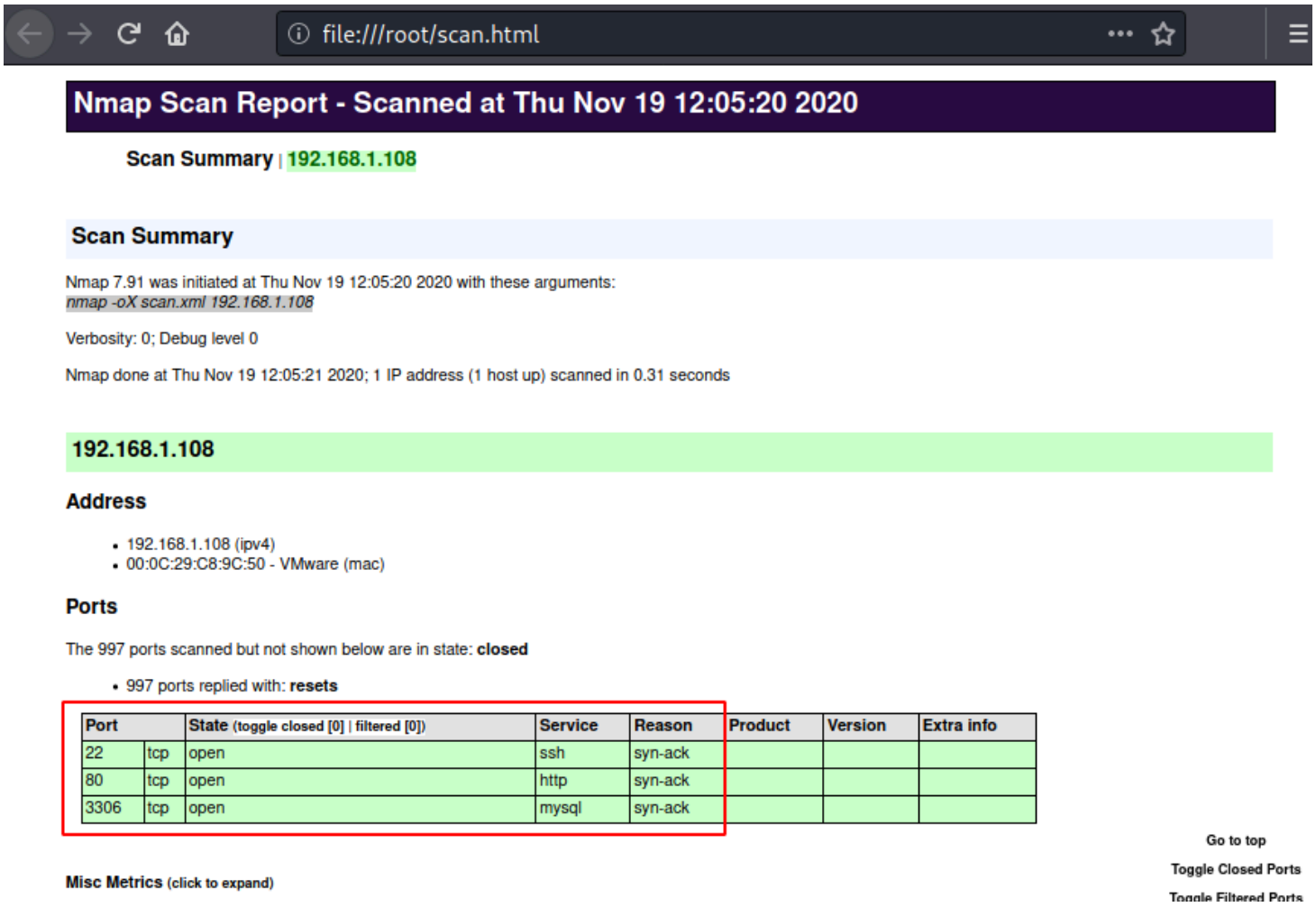
```
root@kali:~# nmap -oX scan.xml 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 12:05 EST
Nmap scan report for 192.168.1.108
Host is up (0.000095s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Sometimes, Pentesters prefer getting an html stylesheet as their report as it gives much-organised scan results:

```
nmap -oX scan.xml --stylesheet=nmap.xsl 192.168.1.108
xsltproc scan.xml -o scan.html
firefox scan.html
```

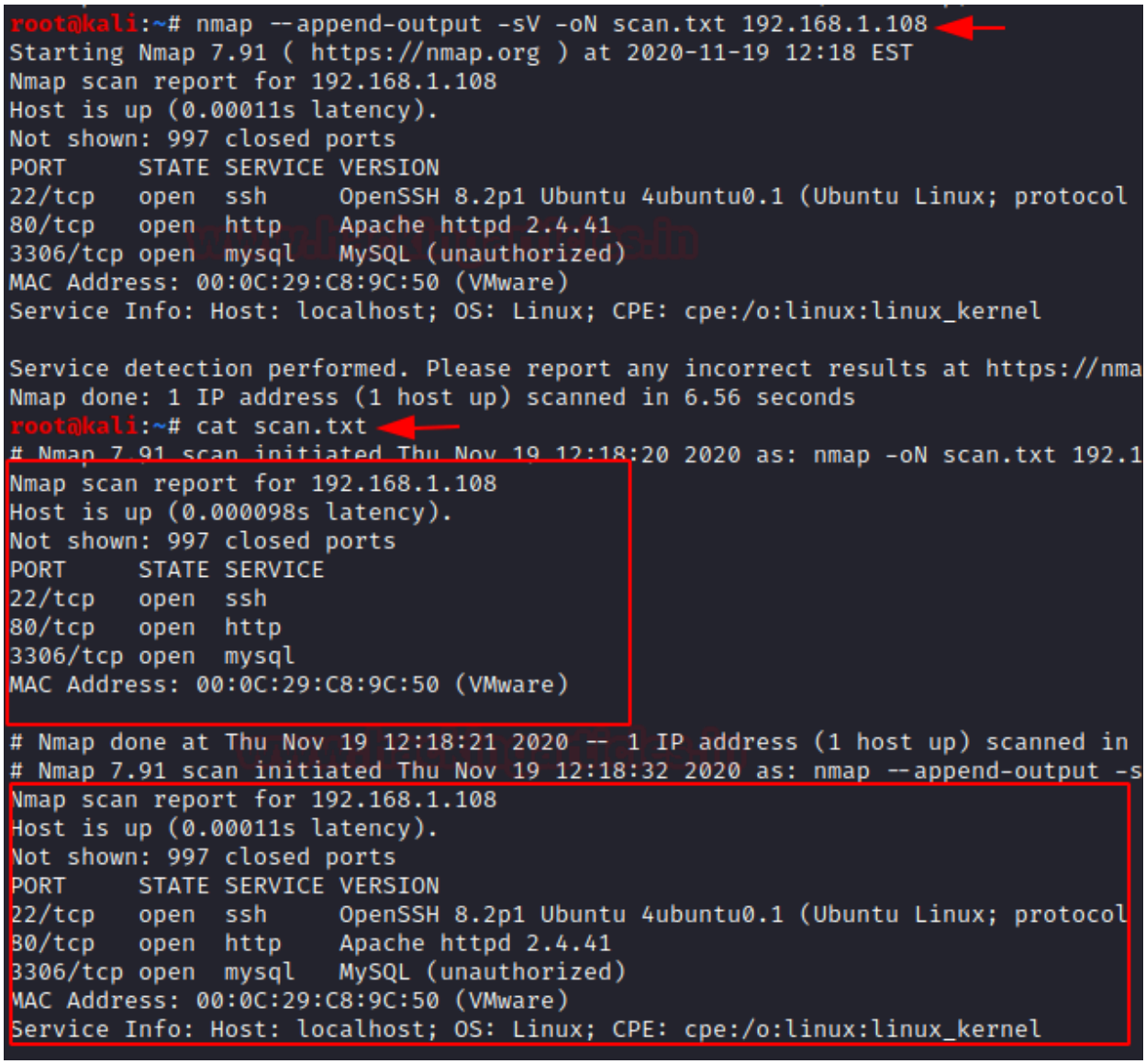
```
root@kali:~# xsltproc scan.xml -o scan.html
root@kali:~# firefox scan.html
```



Appending the output

Nmap by default overwrites logfiles by using any output options. We can use the append option to append the results instead of overwriting them:

```
nmap --append-output -sV -oN scan.txt 192.168.1.108
```



Nmap Scan Report in a grepable format

-oG *<filespec>*

Nmap has different file formats to save the results of a scan. Depending on the needs of the pentester the different formats like the normal, grepable, and XML format can be chosen. The grepable format has been included to help pentester extract information from logs without having the need to write a parser, as this format is meant to be read/parsed with standard Unix tools. It helps in finishing up the scan really quickly.

```
nmap -oG scan.grep 192.168.1.108
cat scan.grep
```

```
root@kali:~# nmap -oG scan.grep 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 12:52 EST
Nmap scan report for 192.168.1.108
Host is up (0.00012s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~# cat scan.grep
# Nmap 7.91 scan initiated Thu Nov 19 12:52:30 2020 as: nmap -oG scan.grep 192.168.1.108
Host: 192.168.1.108 ()  Status: Up
Host: 192.168.1.108 ()  Ports: 22/open/tcp//ssh///, 80/open/tcp//http///, 3306/open/tcp//mysql///
# Nmap done at Thu Nov 19 12:52:31 2020 -- 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~# nmap -oG scan.grep 192.168.1.108 |awk '/open/{print $2 " " $3}'
open ssh
open http
open mysql
root@kali:~#
```

Nmap Scan Report in Alias format

-oA <*filespec*>

Nmap scan has the alias option which saves the scan results in all the formats. The files will be generated with the extensions .nmap, .xml, and .grep.

```
nmap -sV -oA scanme --stylesheet https://raw.githubusercontent.com/honze-net/nmap-
```

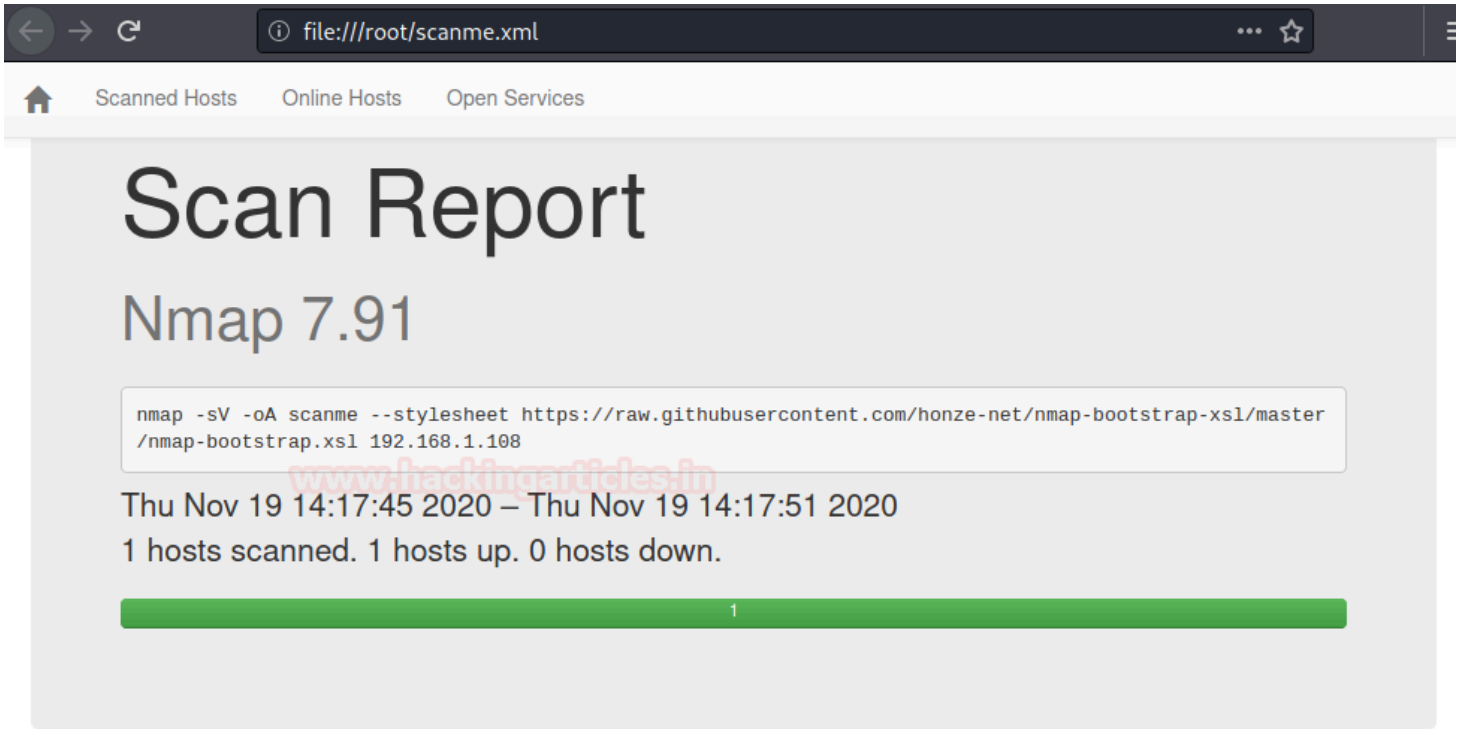
```
root@kali:~# nmap -sV -oA scanme --stylesheet https://raw.githubusercontent.com/honze-net/nmap-bootstrap-xsl/master/nmap-bootstrap.xsl 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 14:17 EST
Nmap scan report for 192.168.1.108
Host is up (0.000094s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Service Info: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds
root@kali:~# firefox scanme.xml
root@kali:~#
```

```
nmap -oA scan 192.168.1.108
```

```
root@kali:~/nmap# nmap -oA scan 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-19 12:00 EST
Nmap scan report for 192.168.1.108
Host is up (0.000085s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:C8:9C:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@kali:~/nmap# ls
scan.gnmap  scan.nmap  scan.xml
root@kali:~/nmap#
```



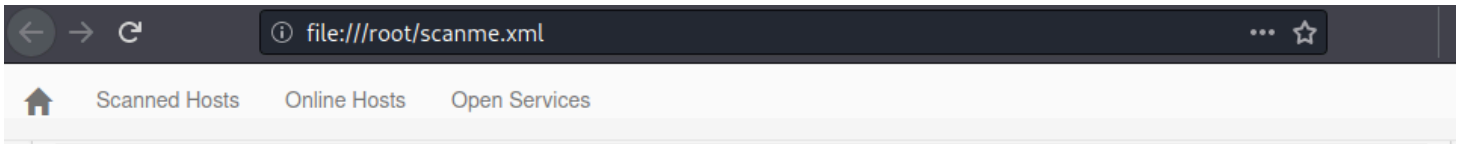
Scanned Hosts

Show 10 entries Search:

State	Address	Hostname	TCP (open)	UDP (open)
up	192.168.1.108		3	0

Showing 1 to 1 of 1 entries Previous 1 Next

Online Hosts



Port	Protocol	State Reason	Service	Product	Version	Extra Info
22	tcp	open syn-ack	ssh	OpenSSH	8.2p1 Ubuntu 4ubuntu0.1	Ubuntu Linux; protocol 2.0
cpe:/a:openbsd:openssh:8.2p1						
80	tcp	open syn-ack	http	Apache httpd	2.4.41	
cpe:/a:apache:http_server:2.4.41						
3306	tcp	open syn-ack	mysql	MySQL		unauthorized
cpe:/a:mysql:mysql						

Open Services

Show 10 entries Search:

Address	Port	Protocol	Service	Product	Version	CPE	Extra info
192.168.1.108	22	tcp	ssh	OpenSSH	8.2p1 Ubuntu 4ubuntu0.1	cpe:/a:openbsd:openssh:8.2p1	Ubuntu Linux; protocol 2.0
192.168.1.108	80	tcp	http	Apache httpd	2.4.41	cpe:/a:apache:http_server:2.4.41	
192.168.1.108	3306	tcp	mysql	MySQL		cpe:/a:mysql:mysql	unauthorized