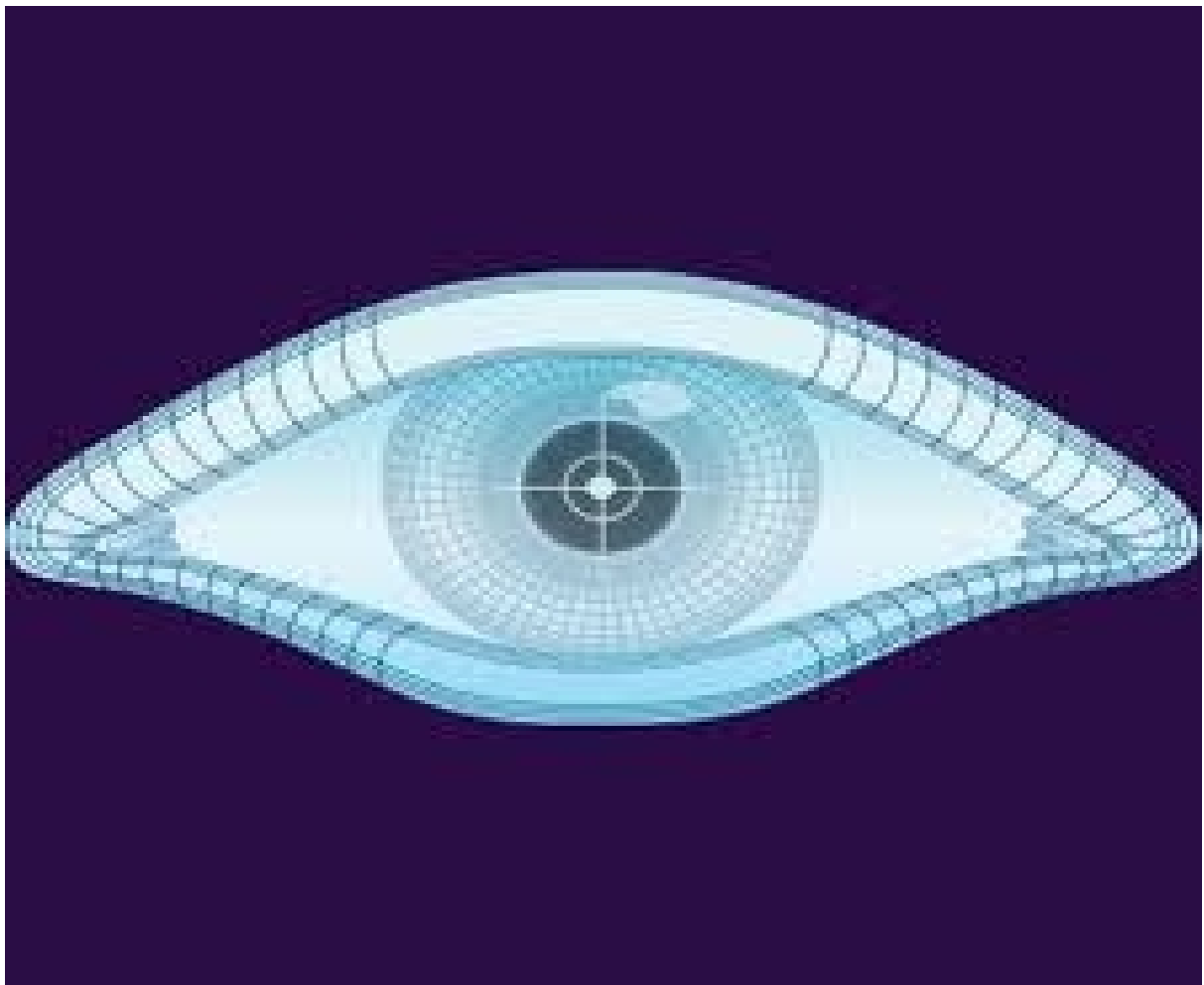


## Nmap Explication and basic arguments



Author : -Bad\_Boy-

## 1. What is Nmap ?

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

source : <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>

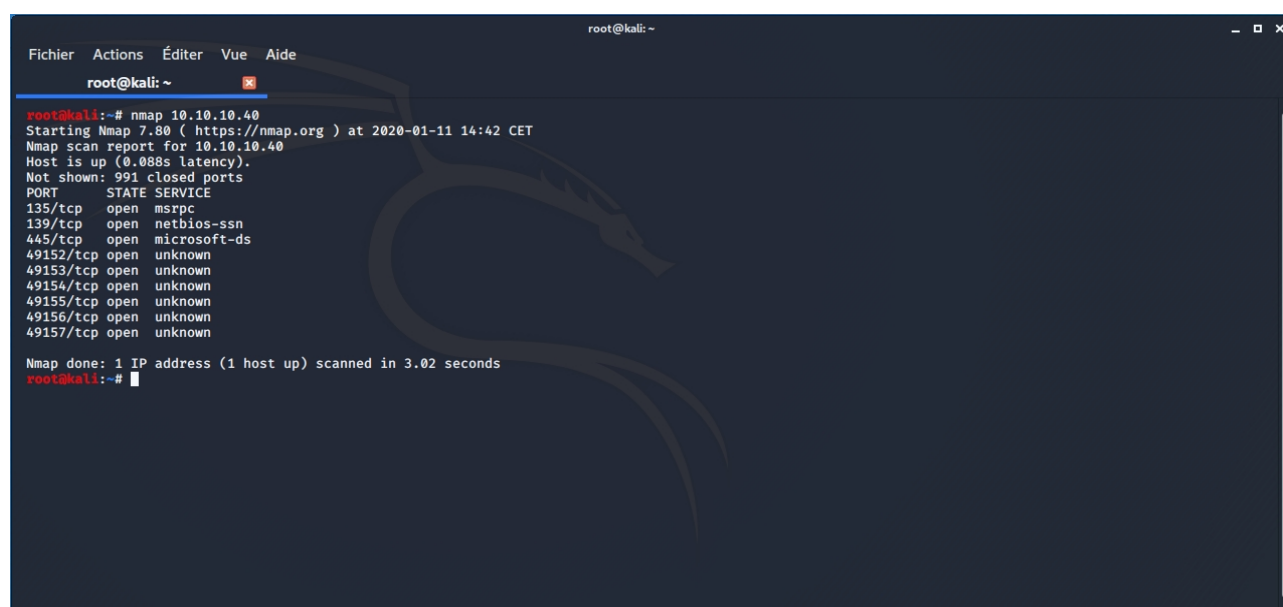
## 2. How to lunch a scan with nmap ?

For this tutorial I'll use the HackTheBox machine called "Blue" because i can't scan a website or something like because it's not very legal... So you got 2 ways to lunch a scan.

First you can lunch an nmap scan with the ip that you want to test like this.

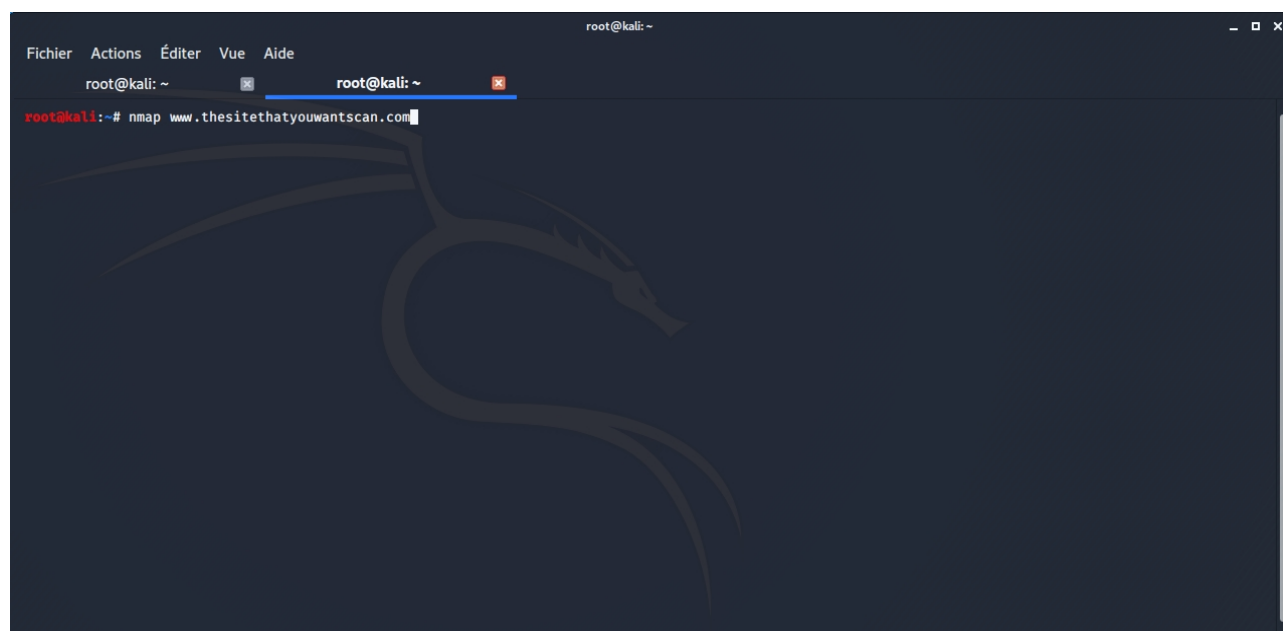
Or you can lunch an nmap scan with the url of a website.

Now let's have more information about the IP or URL.

A terminal window titled 'root@kali: ~' showing the output of an nmap scan. The command 'nmap 10.10.10.40' has been executed. The output includes the Nmap version (7.80), the scan date and time (2020-01-11 14:42 CET), and a list of open ports with their corresponding services. The background features a faint Kali Linux dragon logo.

```
root@kali:~# nmap 10.10.10.40
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-11 14:42 CET
Nmap scan report for 10.10.10.40
Host is up (0.088s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.02 seconds
root@kali:~#
```

A terminal window titled 'root@kali: ~' showing the command 'nmap www.thesitethatyouwantscan.com' being entered. The background features a faint Kali Linux dragon logo.

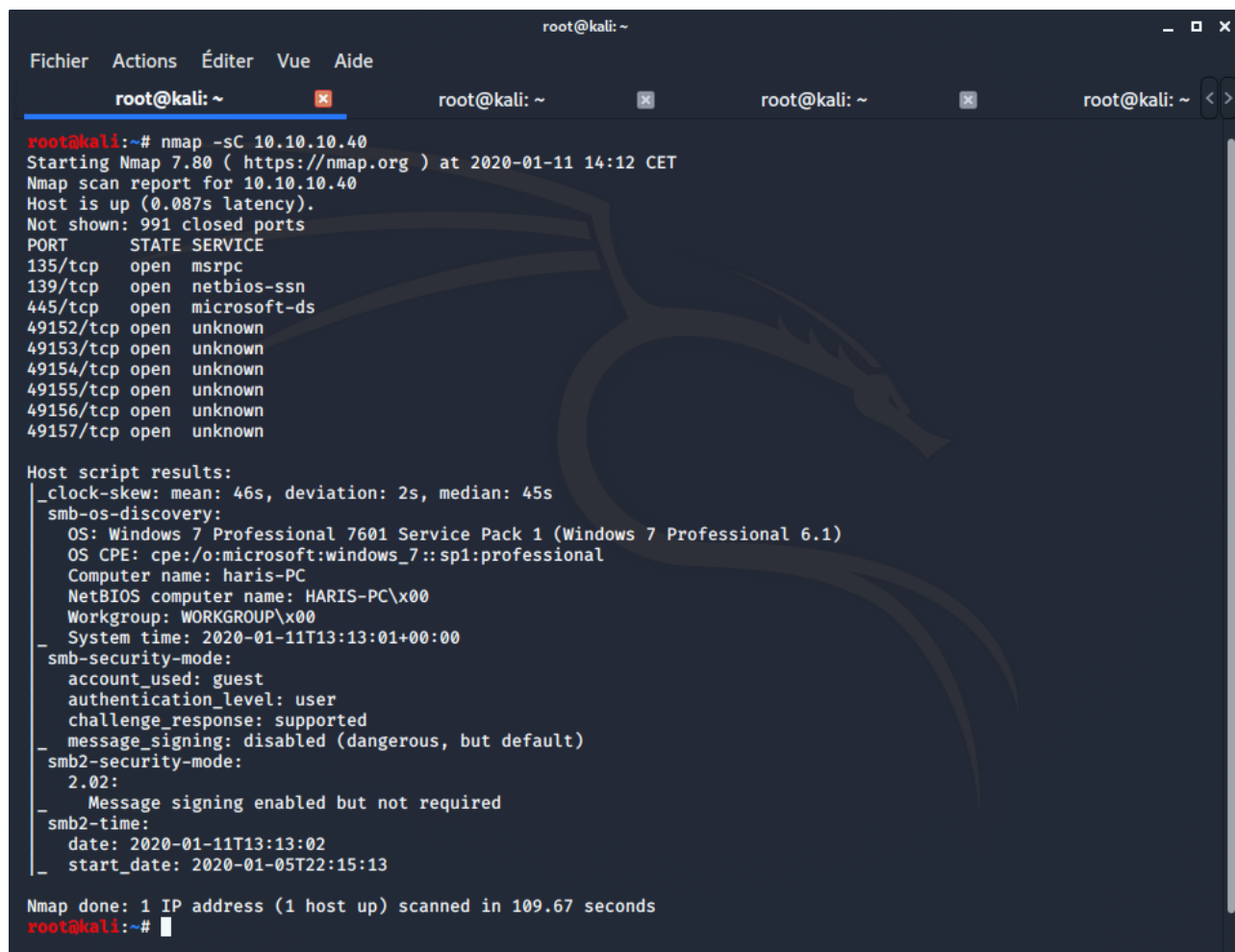
```
root@kali:~# nmap www.thesitethatyouwantscan.com
```

### 3. The -sC argument :

These scripts are the default set and are run when using the -sC or -A options rather than listing scripts with --script. This category can also be specified explicitly like any other using --script=default.

For more explication visit this link : <https://nmap.org/book/nse-usage.html>

Let's try this argument !



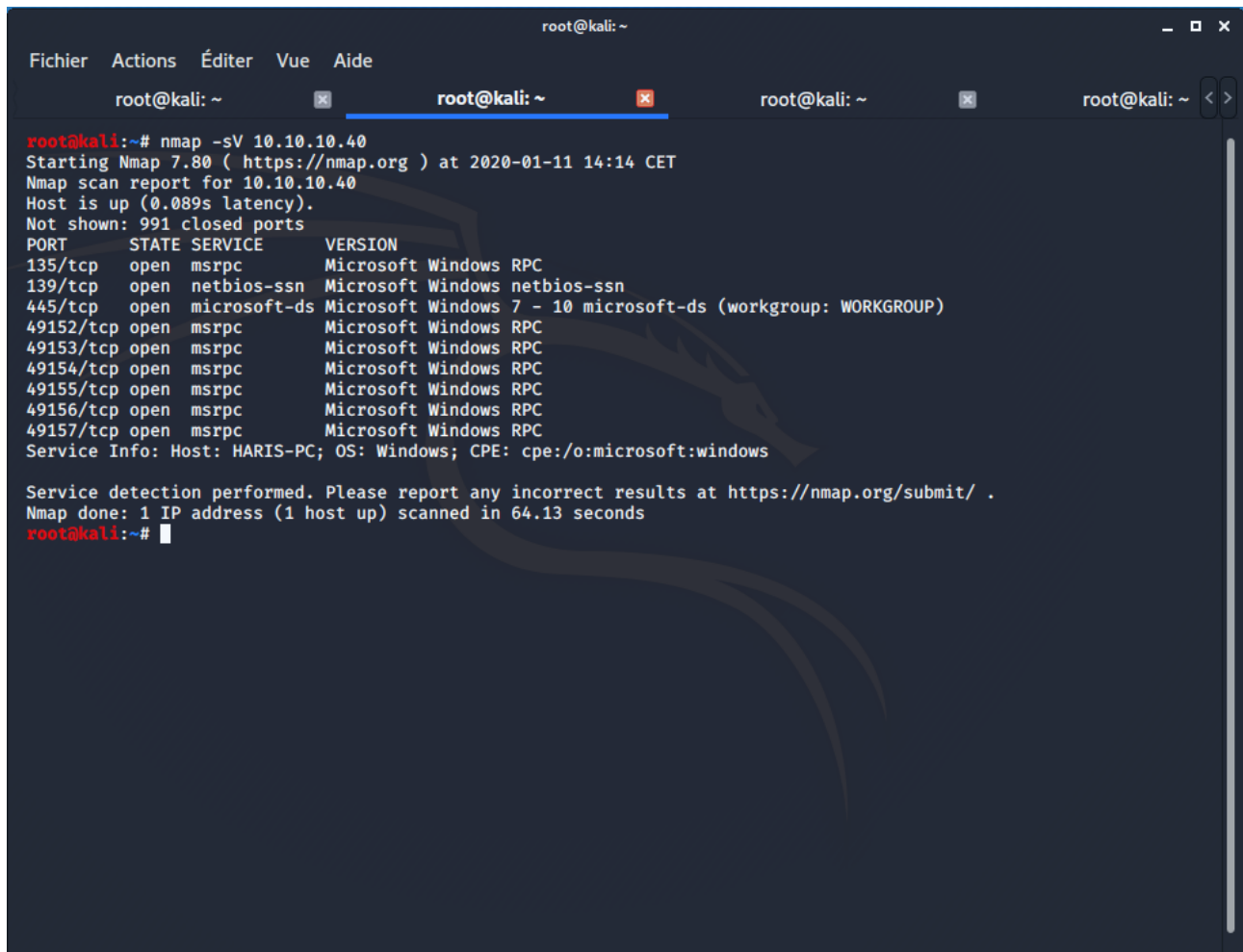
```
root@kali: ~  
Fichier Actions Éditer Vue Aide  
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~  
root@kali:~# nmap -sC 10.10.10.40  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-11 14:12 CET  
Nmap scan report for 10.10.10.40  
Host is up (0.087s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
  
Host script results:  
_clock-skew: mean: 46s, deviation: 2s, median: 45s  
smb-os-discovery:  
  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)  
  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional  
  Computer name: haris-PC  
  NetBIOS computer name: HARIS-PC\x00  
  Workgroup: WORKGROUP\x00  
  System time: 2020-01-11T13:13:01+00:00  
smb-security-mode:  
  account_used: guest  
  authentication_level: user  
  challenge_response: supported  
  message_signing: disabled (dangerous, but default)  
smb2-security-mode:  
  2.02:  
    Message signing enabled but not required  
smb2-time:  
  date: 2020-01-11T13:13:02  
  start_date: 2020-01-05T22:15:13  
  
Nmap done: 1 IP address (1 host up) scanned in 109.67 seconds  
root@kali:~#
```

As you can see we have some information about the OS running on a port but for the moment we don't have all services discover so let's dig more deeper !

## 4. The -sV argument :

Besides determining the state a TCP/UDP port, nmap can also try to figure out which service is listening on that port. This is done by sending different requests to the port, and analyzing the replies. This feature is called service detection, and is activated with option -sV or you can use the -A. ( the argument -A is the ~combination of the -sV and the -sC arguments ).

Use in first the -sV argument :



```
root@kali: ~  
Fichier Actions Éditer Vue Aide  
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~  
root@kali:~# nmap -sV 10.10.10.40  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-11 14:14 CET  
Nmap scan report for 10.10.10.40  
Host is up (0.089s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
49152/tcp  open  msrpc        Microsoft Windows RPC  
49153/tcp  open  msrpc        Microsoft Windows RPC  
49154/tcp  open  msrpc        Microsoft Windows RPC  
49155/tcp  open  msrpc        Microsoft Windows RPC  
49156/tcp  open  msrpc        Microsoft Windows RPC  
49157/tcp  open  msrpc        Microsoft Windows RPC  
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 64.13 seconds  
root@kali:~#
```

As you can see after that we have all services running behind every port !

So now let's try the argument -A :

```
root@kali: ~  
Fichier Actions Éditer Vue Aide  
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~  
root@kali:~# nmap -A 10.10.10.40  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-11 14:17 CET  
Nmap scan report for 10.10.10.40  
Host is up (0.087s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)  
49152/tcp  open  msrpc        Microsoft Windows RPC  
49153/tcp  open  msrpc        Microsoft Windows RPC  
49154/tcp  open  msrpc        Microsoft Windows RPC  
49155/tcp  open  msrpc        Microsoft Windows RPC  
49156/tcp  open  msrpc        Microsoft Windows RPC  
49157/tcp  open  msrpc        Microsoft Windows RPC  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.80%E=4%D=1/11%OT=135%CT=1%CU=42442%PV=Y%DS=2%DC=T%G=Y%TM=5E19CB  
OS:54%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=100%TI=I%CI=I%SS=S%TS=  
OS:7)OPS(O1=M54DNW8ST11%O2=M54DNW8ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11%O5=M5  
OS:4DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=200  
OS:0)ECN(R=Y%DF=Y%T=80%W=2000%O=M54DNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S  
OS:+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%  
OS:T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=  
OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%  
OS:S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(  
OS:R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=  
OS:N%T=80%CD=Z)  
  
Network Distance: 2 hops  
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
_clock-skew: mean: 46s, deviation: 2s, median: 44s  
smb-os-discovery:  
  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)  
  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional  
  Computer name: haris-pc  
  NetBIOS computer name: HARIS-PC\x00  
  Workgroup: WORKGROUP\x00  
_ System time: 2020-01-11T13:19:54+00:00  
smb-security-mode:  
  account_used: guest  
  authentication_level: user  
  challenge_response: supported  
_ message_signing: disabled (dangerous, but default)  
smb2-security-mode:  
  2.02:  
_ Message signing enabled but not required  
smb2-time:  
  date: 2020-01-11T13:19:52  
_ start_date: 2020-01-05T22:15:13  
  
TRACEROUTE (using port 111/tcp)  
HOP RTT ADDRESS  
1 87.55 ms 10.10.14.1  
2 87.66 ms 10.10.10.40
```

We can see that the argument -A is a combination of the -sC and the -sV but with a little things plus, we have the tcp/ip fingerprint and the TraceRoute.

## 5. The vulnerable script

The last point of my "tutorial" is the vulnerable script, The way NSE scripts are based on a list of predefined categories. These categories include: auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln. Vuln is the one that you'll be using to launch for scanning vulnerable subdomains.

```
root@kali: ~  
Fichier Actions Éditer Vue Aide  
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~  
root@kali:~# nmap -sC -sV -A --script vuln 10.10.10.40  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-11 14:26 CET  
Pre-scan script results:  
| broadcast-avahi-dos:  
|   Discovered hosts:  
|     224.0.0.251  
|   After NULL UDP avahi packet DoS (CVE-2011-1002).  
|_ Hosts are all up (not vulnerable).  
Nmap scan report for 10.10.10.40  
Host is up (0.087s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
49152/tcp open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
49153/tcp open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
49154/tcp open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
49155/tcp open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
49156/tcp open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
49157/tcp open  msrpc        Microsoft Windows RPC  
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.80%E=4%D=1/11%OT=135%CT=1%CU=40536%PV=Y%DS=2%DC=T%G=Y%TM=5E19CD  
OS:7C%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS  
OS:=7)OPS(O1=M54DNW8ST11%O2=M54DNW8ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11%O5=M  
OS:54DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=20  
OS:00)ECN(R=Y%DF=Y%T=80%W=2000%O=M54DNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=  
OS:S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y  
OS:%T=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%O=0%F=R%O=%RD  
OS:=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0  
OS:%S=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1  
OS:(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI  
OS:=N%T=80%CD=Z)  
  
Network Distance: 2 hops  
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_ smb-vuln-ms10-054: false  
|_ smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND  
|_ smb-vuln-ms17-010:  
|   VULNERABLE:  
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)  
|     State: VULNERABLE  
|     IDs: CVE:CVE-2017-0143  
|     Risk factor: HIGH  
|     A critical remote code execution vulnerability exists in Microsoft SMBv1  
|     servers (ms17-010).
```

As you can see nmap found an exploit



```
Host script results:
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).
```

So if you check on <https://www.exploit-db.com> you can see that the exploit exist ( ms17-010)

---

This Document is for educational purposes I do not encourage anyone to use this article for illegal actions. Stay on the right track

So It's finish thanks to read my article and enjoy ! Good bye see you soon :)

My HTB profile : <https://www.hackthebox.eu/home/users/profile/66952>

My Youtube Channel :

[https://www.youtube.com/channel/UCANZaRZztsKsVYA\\_SoxanaQ](https://www.youtube.com/channel/UCANZaRZztsKsVYA_SoxanaQ)

-Bad\_Boy-