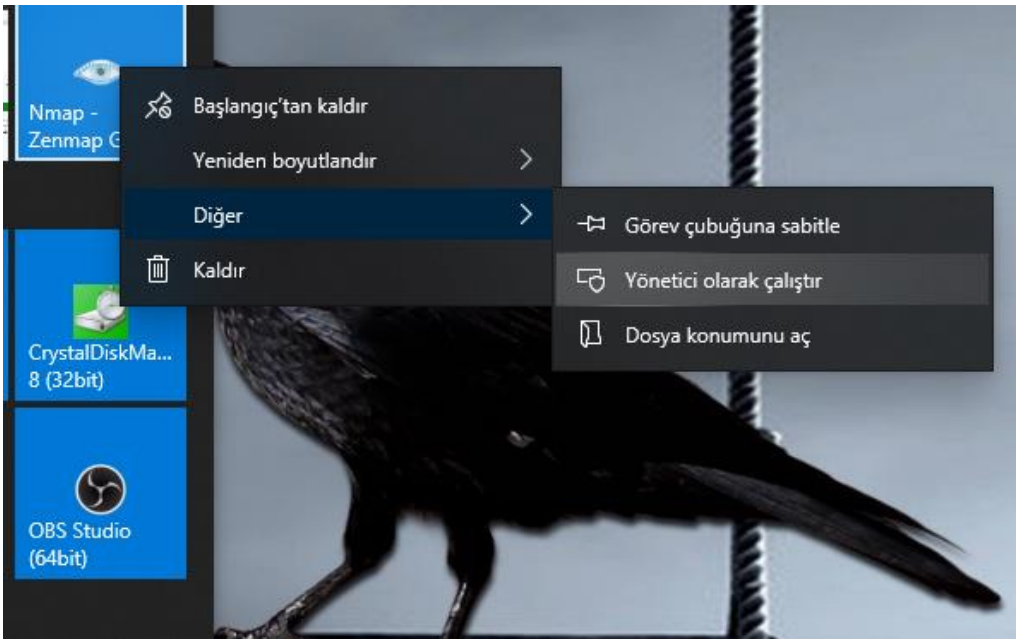
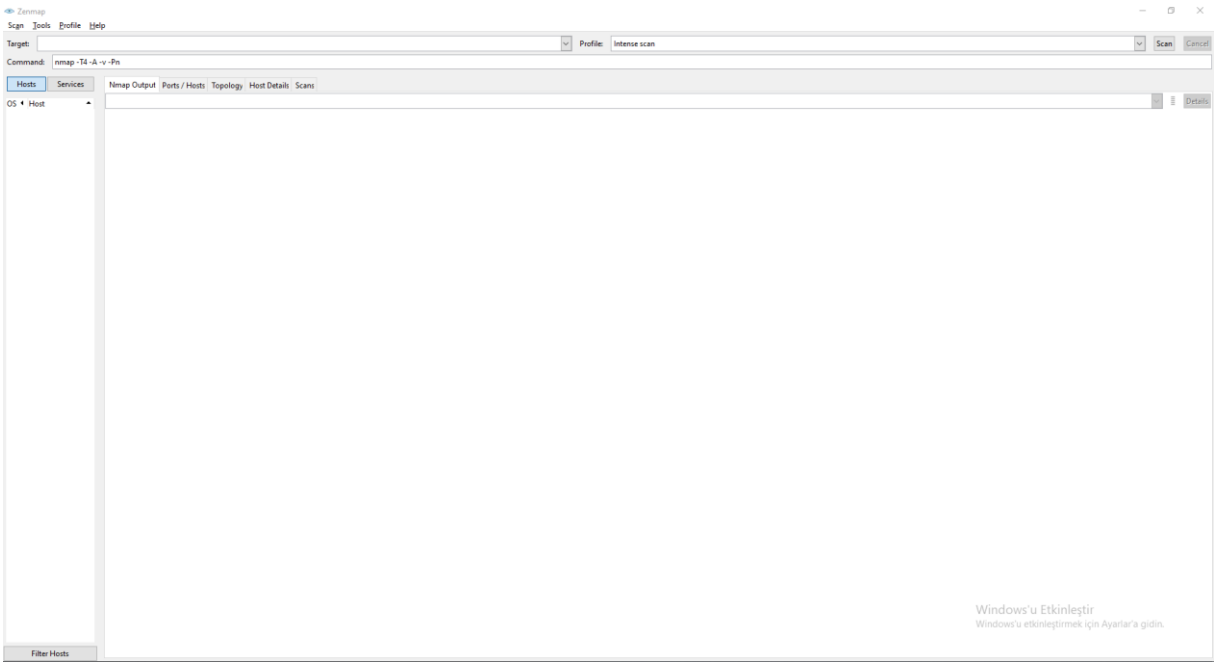
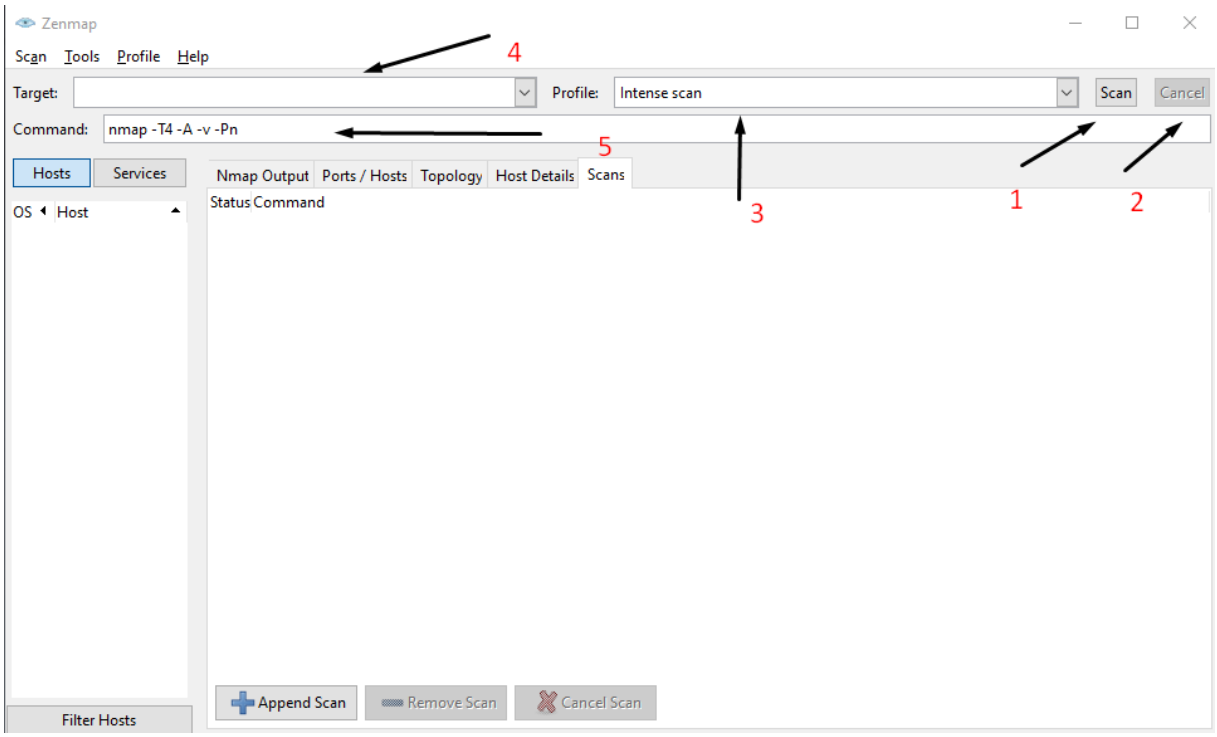


When you start to use zenmap you should run zenmap as run as administrator.

(This is also called root, also in the linux platform you should need root as a user.)



When you open the Zenmap you will see empty page like that.



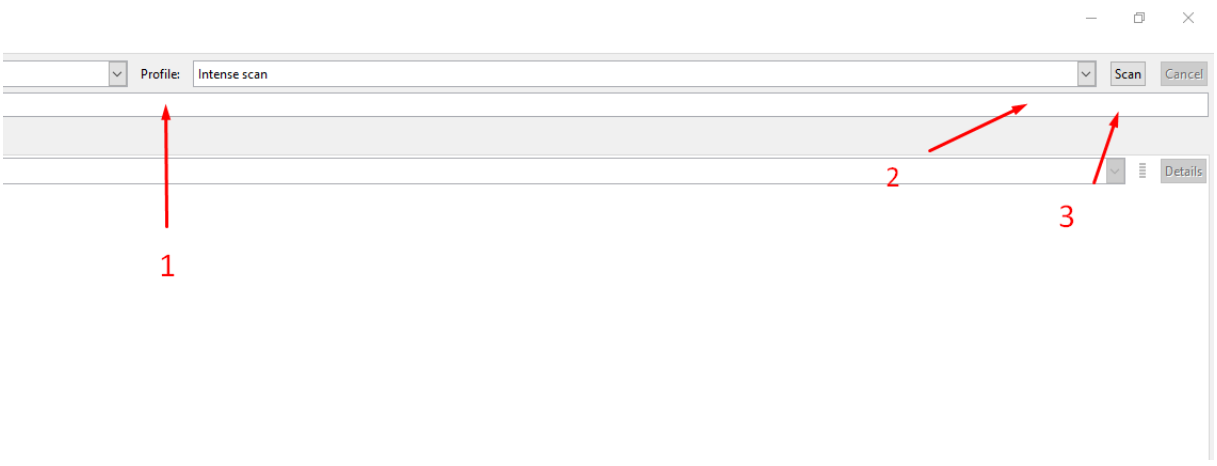
If you want tos can a network or ip adress you have two chooses. First of them you can use preparedprofiles. As you can see in the Picture a gave some numbers, now I will explain meaning of these numbers.

1 is scan button,when you want to scan any network, ip adress etc. You should press that button and you can cancel with number 2.

You will choose your target from number 4 but do not forget you could not write with http:// when you use this part zenmap will not Show any details to you. You shuld write directly your target website or ip adress.

In number 3, you can use prepared profiles and also you can see if you add any profile by yourself in there.

Also, when you choose target and profile, at the command side (number 5) you will see commands. There are the commands you need to enter when you use nmap.



Now I will write prepared profiles.

Intense Scan

(-T4) is an option for timing which ranges from 0–5, where 0 is the slowest and 5 is the fastest.

(-A) is an option that determines the type of OS and it's versions. Along with the output.

(-v) is an option that gives feedback as Nmap makes progress in the scan.

This scans the most common TCP ports quickly and also determines the OS type, their services as well as versions

1. Intense Scan plus UDP

sS tells Nmap to scan TCP ports using SYN Packets.

-sU is an option that scans UDP ports as well.

This works as regular intense scan but, also scans UDP Ports.

2.Intense Scan, all TCP Ports

Since, it takes time to scan all the ports, Nmap usually scans top 1000 most common ports. However, ***Intense Scan, all TCP Ports*** *asks Nmap to scan all the ports from* ***1–65535(max)***.

3.Intense Scan, no ping

-Pn assumes that the host is up.

This works exactly similar to other Intense scan. However, this assumes that the host is up. This scan is basically helpful when the target is blocking ping request and you know that the target is up.

4.Ping Scan

This command only pings the target but does not scan any port.

5.Quick Scan

Here, **-F** is an option for fast scan. Instead of scanning all the ports, it only scans few ports.

This command scans only limited number of TCP ports. i.e. Top 100 most common TCP ports.

6.Quick Scan

Here, **-F** is an option for fast scan. Instead of scanning all the ports, it only scans few ports.

This command scans only limited number of TCP ports. i.e. Top 100 most common TCP ports.

7.Quick Scan Plus

Here, **-O** is an option that detects the type of OS, then performs light scan.

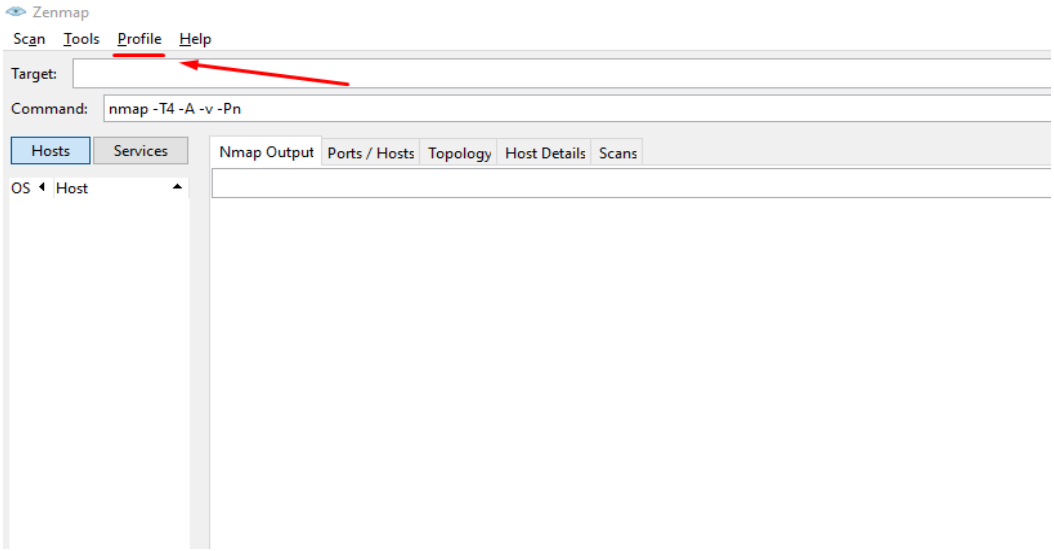
8.Quick Trace Route

Traceroute: Traceroute is a program that records the route between your computer and certain destination through Internet.

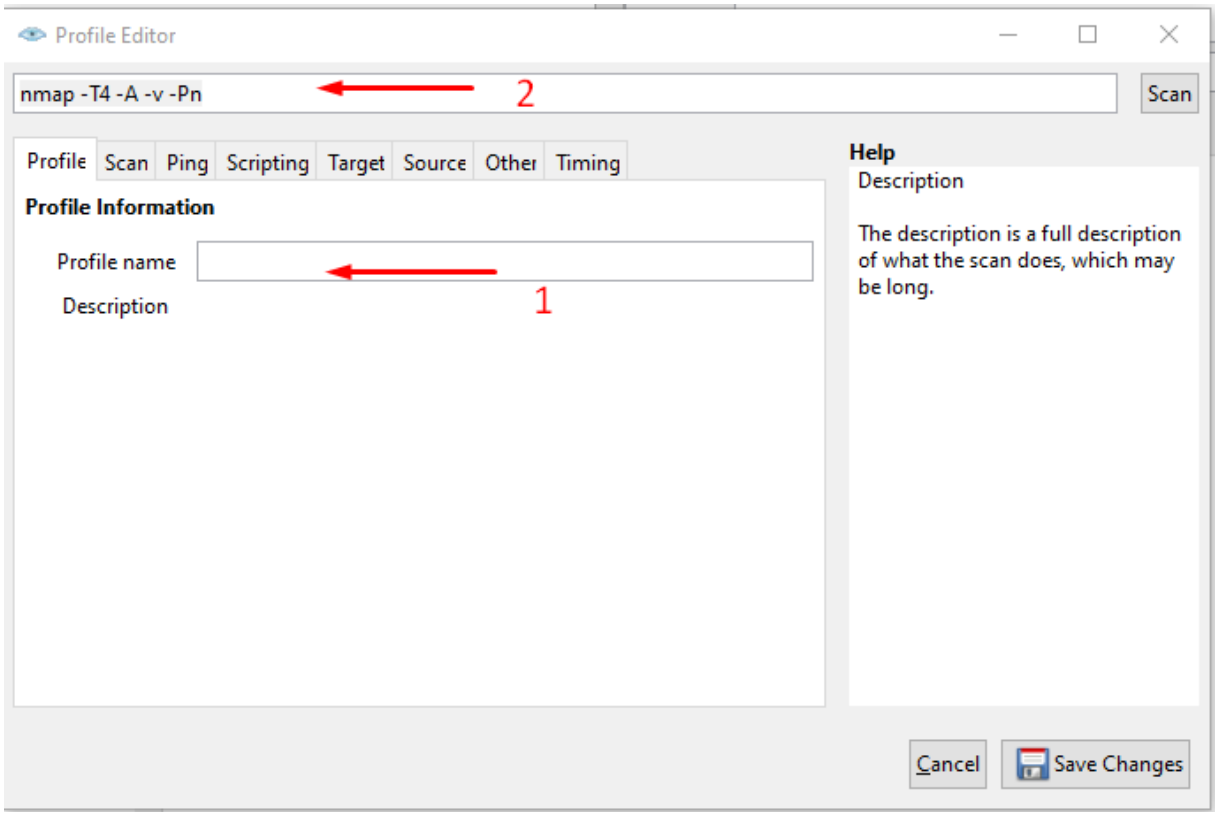
This command will traceroute and ping all the hosts defined in a target.

9. Regular Scan

This command will issue a TCP SYN scan for the most common 1000 ports using ping request for host detection.



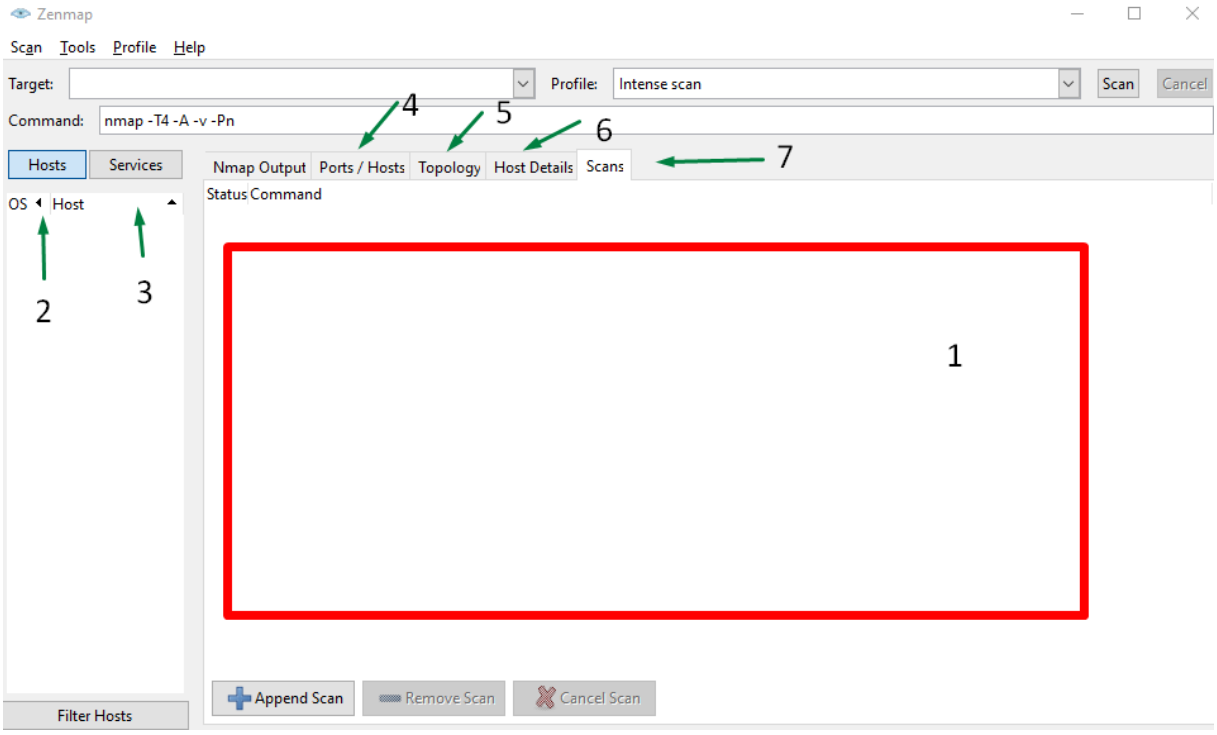
The secon choose is you can add a profile by yourselves. As you can see in the Picture when you click the profile button you will see two options. One of them is add new profile and secon of them is edit the profiles.



As you can see, first page of the profile editor there are two part. Number 1 is profile name, you can give a name your profile and you can see the commands at number two.

I explained other details above which are profile types section. However I will expain one part which are timing templete. I took a table from nmap.org a table , this table expalin many details about that time part. Also I shold say shortly timing tamplete part between T0 and T5. T0 is the slowest, but also the most detailed. the fastest is T5

	T0	T1	T2	T3	T4	T5
Name	Paranoid	Sneaky	Polite	Normal	Aggressive	Insane
`min-rtt-timeout`	100	100	100	100	100	50
`max-rtt-timeout`	300,000	15,000	10,000	10,000	1,250	300
`initial-rtt-timeout`	300,000	15,000	1,000	1,000	500	250
`max-retries`	10	10	10	10	6	2
Initial (and minimum) scan delay (`--scan-delay`)	300,000	15,000	400	0	0	0
Maximum TCP scan delay	300,000	15,000	1,000	1,000	10	5
Maximum UDP scan delay	300,000	15,000	1,000	1,000	1,000	1,000
`host-timeout`	0	0	0	0	0	900,000
`min-parallelism`	Dynamic, not affected by timing templates					
`max-parallelism`	1	1	1	Dynamic	Dynamic	Dynamic
`min-hostgroup`	Dynamic, not affected by timing templates					
`max-hostgroup`	Dynamic, not affected by timing templates					
`min-rate`	No minimum rate limit					
`max-rate`	No maximum rate limit					
`defeat-rst-ratelimit`	Not enabled by default					



Now, I will explain last part shortly. Number 1 part is called nmap output, at that part we can see many details about scan but this part generally so mixed.

At number two called hosts we can see connected devices at the network and we can see at the number three (services part) the used services which are used by these connected devices.

At number 4(port/host) part we can see the open, closed and filtered ports of the device in the target ip address.

In the part 5 we can see topology of the target network or devices. (for ex. We can see all connected devices topology at the network or we can see path of the Internet connection to connect target ip address.

In the number 6 we can see more detail about hosts/devices and we can see even operation systems of the devices.

In the part 7 we can see history of scan.(all scanned ip addresses which are scanned.)