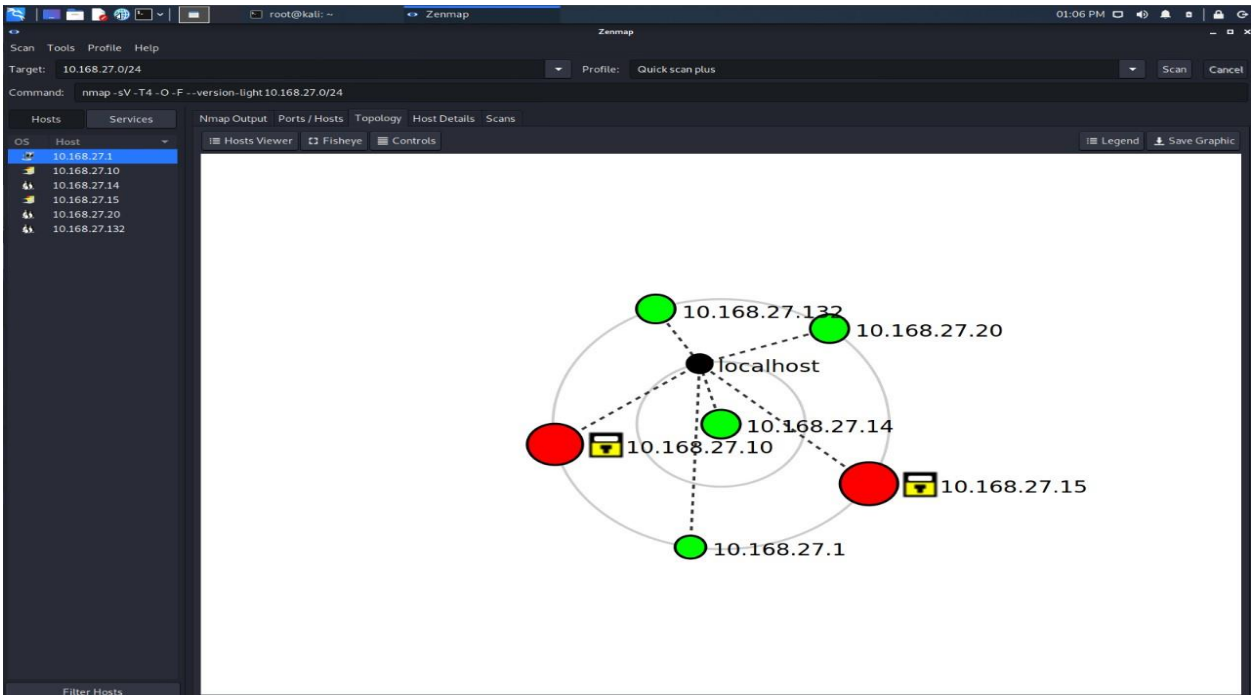

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

```
nmap -sV -T4 -O -F --version-light 10.168.27.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-31 20:35 MDT
Nmap scan report for 10.168.27.10
Host is up (0.00061s latency).
Not shown: 92 filtered ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:80:6F:38 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.168.27.14
Host is up (0.00043s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:11:0B:E5 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.168.27.15
Host is up (0.00057s latency).
Not shown: 90 filtered ports
PORT      STATE SERVICE       VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime       Microsoft Windows USA daytime
21/tcp    open  ftp           FileZilla ftpd
80/tcp    open  http          Microsoft IIS httpd 8.5
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)
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:15:5D:01:80:07 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
```

While running Nmap in analyzing the results the following topology seems to be a star depicted in the first image. There are 6 machines connected to the local host 10.168.27.1. There are three Linux machines all using the same version of the same operating system 2.6.32 the following IPs are 10.168.27.14, 10.168.27.15 and 10.168.27.132. There are two windows servers using two different versions of the same operating system. Windows sever 2012 for 10.168.27.10 and windows sever 2008 for 10.168.27.15. The last this time seems to be some sort of unidentifiable machine. This sort of topology is indicative of a centralized environment which benefits and streamlines administration.

IP 10.168.27.10 has quite a bit of open ports which could lead to some security issues. Port 389 TCP is one and has a found vulnerability **CVE-2022-0918** A vulnerability was discovered in the 389 Directory Server that allows an unauthenticated attacker with network access to the LDAP port to cause a denial of service. The same IP also has port 445 open which has a Vulnerability associated with windows XP port 445 open allows remote attackers to cause a denial of service (CPU consumption) via a flood of TCP SYN packets containing possibly malformed data **CVE-2002-0283.**