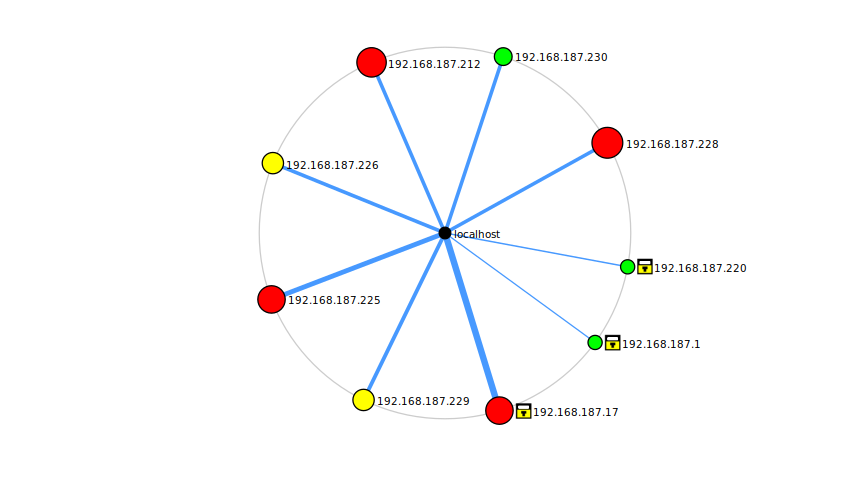
Task 1:

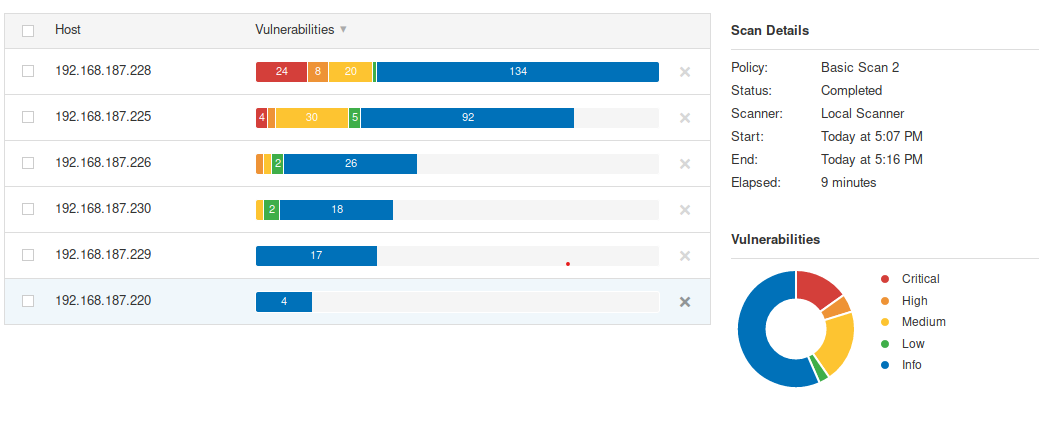
| IP | OS | Services | Open ports(total) | topology |
| --- | --- | --- | --- | --- |
| 192.168.187.1 | N/A |  | 0 | Image below graph |
| 192.168.187.17 | Microsoft Windows server 2016 | domain, kerberos-sec, kpasswd5, idap, microsoft-ds, msrpc, ms-wbt-server, ncacn\_http, netbios-ssn, tcpwrapped | 12 | Image below graph |
| 192.168.187.212 | Microsoft Windows 8.1 | domain, kerberos-sec, kpasswd5, idap, microsoft-ds, msrpc, ms-wbt-server, ncacn\_http, netbios-ssn, tcpwrapped | 18 | Image below graph |
| 192.168.187.220 | N/A |  | 0 | Image below graph |
| 192.168.187.225 | Linux 2.6.x | ajp13, domain, ftp, http, mysql, netbios-ssn, postgresql, smtp, ssh, telnet | 12 | Image below graph |
| 192.168.187.226 | Linux 2.4.x | rpcbind, ssh, status | 3 | Image below graph |
| 192.168.187.228 | Microsoft windows XP | Afp, chargen, daytime, discard, domain, echo, ftp, http, https, microsoft-ds, msdtc, msrpc, ms-wbt-server, netbios-ssn, wins | 24 | Image below graph |
| 192.168.187.229 | Microsoft windows XP | microsoft-ds, netbios-ssn, msrpc, printer, qotd, smtp | 3 | Image below graph |
| 192.168.187.230 | Linux 2.6.x | ssh | 1 | Image below graph |

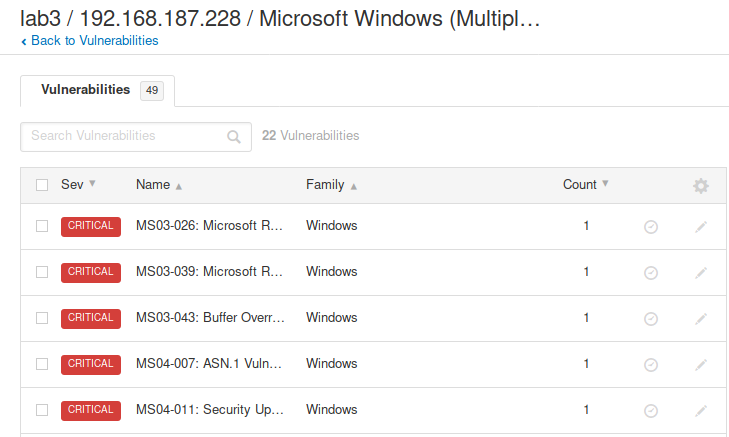
Image of topology

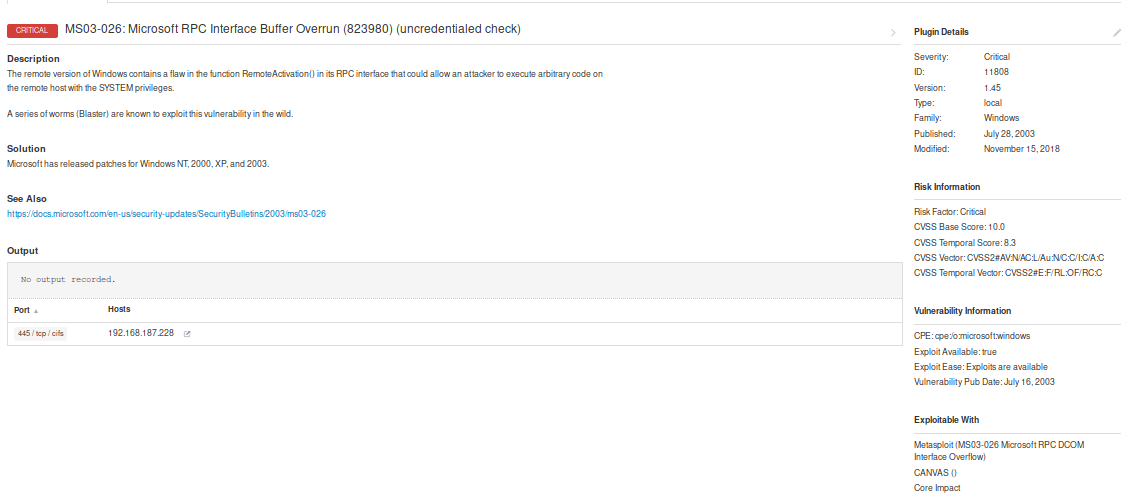


Task 2:

Scan took 9 minutes and shows many critical vulnerabilities. Some examples can be found in the IP 192.168.187.228 which show quite a few critical points in un updated windows patches.





MS03-026:Microsoft RPC Interface Buffer Overrun(823980)

Buffer overrun could run attackers' choice of code and allow for code execution. This vulnerability, if exploited, allows an attacker to gain complete control over a remote computer. This would allow the attacker the ability to take any action on the server. Some actions are, changing web pages, or adding new users. A series of worms(blastors) are known to exploit this.

To carry out such an attack, an attacker would require the ability to send a malformed message to the RPC service and thereby cause the target machine to fail in such a way that arbitrary code could be executed.(https://docs.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-026)

Exploit: (<https://vulners.com/nessus/MSRPC_DCOM.NASL>)