**NESSUS Scan**

The Nessus scan was conducted on day 0.

The dataset consists of security vulnerabilities associated with the computers on the workstation subnet.

The ground truth states that five machines 192.168.2.171 through 192.168.2.175 are unpatched. The security hold is that arbitrary code can be executed on the remote host through the Microsoft GDI rendering engine. **According the defined network rules, no remote access should be allowed on all the computers on the corporate's network.**

**Using a graph-based approach, I think I will need to write a parser that links IP to security message. Since majority of the machines scanned by Nessus does not return the above code (the majority of the data returned are another minor security concern), the anomaly should be detected.**

**Firewall**

*Day 1*

DOS attack started at 1139 and ended at 1251.

External systems are attempting to disrupt communication with the web server. Machines with IPs of 10.200.150.x/24 DOS 172.20.1.5 (web server)

**My thoughts:** "Each internet device should be represented as separate nodes since it will look like there are multiple devices requesting a lot of transaction instead of a since device requesting a lot of transaction."

*Day 2*

Port scan 1056 – 1228, workstation to server

Socially engineered attack:

SMTP email at 1123 (first email) and 1323 (response email) - email exchanged between AFC employees

* + - Not sure how to detect this

Remote desktop connection 1331 – violation of corporate policy.

Priority flag is raised in the firewall log

*Day 3*

Undocumented computer on the workstation subnet with IP of 192.168.2.251 which is undocumented. At 14:06

**IDS**

*Day 1*

Dos attack started at 1139 and ended at 1143.

Flags the DOS attacks logged by the firewall. Small time delay for IDS to process events.

Port scan 1115 – 1141

Workstation computers begins port scanning other systems on their own subnet (does not pass through firewall so firewall cannot detect the port scan)

*Day 2*

Port scan 0901 – 927 on subnet (workstation subnet only, not detected by the firewall)

Port scan 1056 1228 port scan attack form the unpatched workstations, across subnets (firewall capture this data).

*Day 3*

**Security Log**

*Day 2*

*Social engineered attack*

*Authentication to the domain controller for the web server at 1331*