ITSC 303

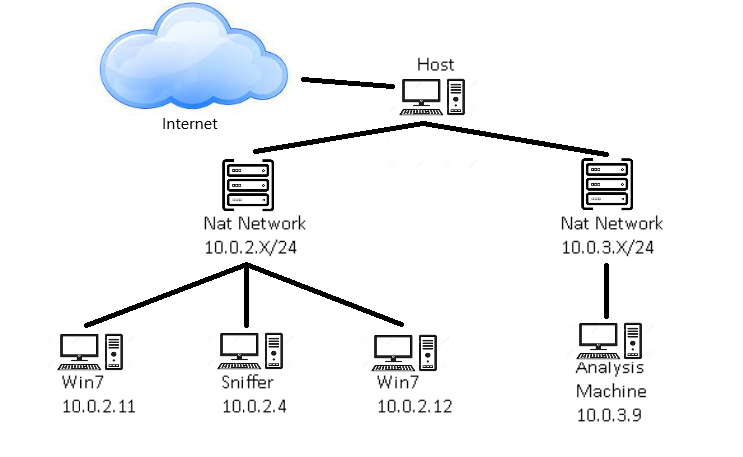
Malware Analysis

Final Project - Weekly Report 2

D’Artagnan Boocock & Coleton Sanheim

28/03/2022

**Network Topology Diagram:**

****

The host machine is connected to the internet and has two different virtual NAT networks isolated from each other.

The Analysis Machine will be used to perform most of the static analysis.

The Win7 machines will be used to observe how the malware propagates across a network, with the Sniffer Machine observing the network activity.

**Analysis Tools:**

AV/AM tools – MalwareBytes, BitDefender, AVG

Sandbox tools – RegShot

Debugger tools – Ollydbg, Immunity Debugger, windbg (for kernel mode debugging)

Packet capture tools – Wireshark

Disassembler tools – Ghidra, Cutter

Packing programs – UPX, PEiD (for unpacking)

Decompiler tools – JustDecompile, JetBrains

Note that these tools may be subject to change as during analysis we may discover that a tool is not useful in this case or another tool may be required that we did not consider here.