Track B Challenge Guide

Mission Statement

The MakeStuff Company is a medium-sized manufacturing company which specializes in 3D printing. Because the company was focused on their product manufacturing goals, their attention to their cyber infrastructure has been lacking since company inception.

Goal

You are tasked with helping the MakeStuff Company perform various aspects of a cyber infrastructure assessment. These tasks will include Vulnerability Assessment and Exploitation, Cyber Attack Analysis, and Software Analysis/Development. Your actions may be required to take place from either an internal or external network perspective.

The goal of the assessment for the MakeStuff Company is to discover vulnerabilities in their information technology systems by analyzing their environment, carrying out attacks manually or with code, and analyzing ongoing attacks using code.

Perform all the tasks you are assigned to facilitate a successful assessment.

Scope

The in-scope internal systems are located on the 172.16.20.0/24 subnet. This subnet will include the Domain Controller, Email Server, Octoprint 3D Printing Management Server, Company Services Database, Git Server, and user workstations.

In-scope DMZ systems are located on the 172.16.30.0/24 subnet. This subnet includes their website and chat server.

The WAN port IP address of the MakeStuff router is 130.44.210.8/24.

Topology

This scenario utilizes a common topology. This means several things:

- All challenges will use the same VMs. All VMs are deployed when the first challenge is launched (you may launch any challenge first). New VMs will not be deployed when a new challenge is started.
- Changes to a VM in one challenge will remain when accessing the same VM from another challenge
- You will be able to access all available VMs from any challenge. Some challenges require use of certain VMs. Other challenges are able to be solved using any VM you can access.

Credentials

VM Name	Username	Password
DomainUser	Makestuff\\GLEN_DUKE	Tartans@1!
KaliLan	user	tartans
KaliWan	user	tartans
Kali-Target	user	tartans