CCDC Practice Scenario 1

Scenario Author: Chris Morales

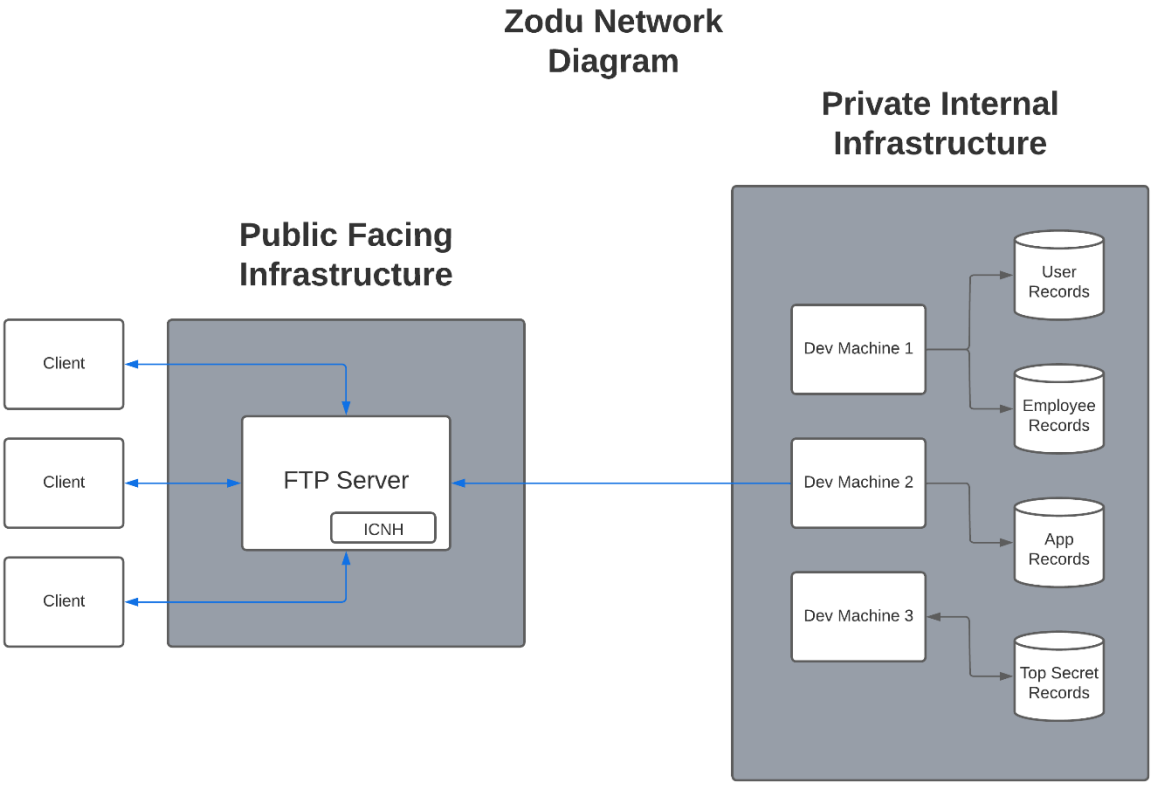
Difficulty: Easy

Tip: Think high-level and *BASICS*

Overview:

You have been contracted to a small business called Zodu. They are a very new company that is only focused on getting their app "Insert Creative Name Here (ICNH)" onto the market and available to be downloaded. Your job is to analyze the existing infrastructure of the company and to provide your input to their IT team regarding their security.

The general overview of their network is shown below:



Upon gathering information from the IT team, the flow of their application deployment was developed as follows:

Internal Workflow:

The main developer *innocentdev* is responsible for uploading the executable (ICNH.exe) to a public location that would allow the customers to download it. And so, they had asked their friend *onestaradmin* who is a system administrator to assist him in achieving this. *Onestaradmin* has had experience creating FTP services and since the goal of the CEO is to make the executable readily available for the customers without needing extra steps to download the app, he created an FTP server. This is the extent of what the IT teams knows about the server.

So now, we gathered information from *onestaradmin* and he had expressed that he didn't have security in mind because there wasn't any sensitive information on the server. And so, to make his job easier, he had removed some security features to gain access into the server and to get the FTP service running quickly to get the company's app up and running. He had explained that the server's executable file will be updated every workday at 5pm from *innocentdev*'s machine. (The team has increased the frequency of the uploads to every 2 minutes for your analysis.)

Public FTP Server:

The FTP server simply accepts FTP connections from customers, and they can simply get the file onto their machines for usage. According to *onestaradmin*, anonymous connections are allowed so users don't need to go through a log-in page. It is assumed that the IP address of the server will not be spread by their *loyal* customers.

Assignment:

Now that you've been given all this preliminary information, you should now be able to perform an analysis of the infrastructure. You are given a subset of the infrastructure. Just the very relevant pieces of information. Specifically, you are given the FTP server, Dev Machine 2 and an Ubuntu machine to perform your penetration testing (install tools as you see fit). You can only attack the machine using information gained from the FTP server from the attacker machine.

Your created machines are as follows:

I'm assuming that you had installed this scenario using my Docker files, scripts, etc

1) **FTP Server:** The hostname/name of the container are "ftpserver".
2) **Developer Machine 2:** The hostname/name of the container are "developer"
3) **Ubuntu Pen-Testing Machine:** The hostname/name of the container are "attacker"

To get into the machine, just use "docker exec –it <container name> bash". Replace "<container name>" with the name of the machine that you want.

Goal: Find a way to access *innocentdev's* machine and gain access to the company's internal network FROM the attacker machine only. So, log into the attacker machine and start testing. Document your full process as to how you got into Developer Machine 2.