**Sensitive Data**

**Key logging**

I would use Social engineering to befriend an administrative or maintenance employee. I would choose them because they are most of the time they are easier to access.

Once I have built that trust with the employee, I would insert a key logger onto their system to capture their keystrokes for about a week. I would then come back and remove the keylogger and review the information provided for the user's keystrokes.

**Security Policies**

**Configured Wireless Networks and Keys**

First I would find a target to attack. I would do this in the parking lot of the target facility. I would get a wireless card or WiFi adapter and use Airmon-NG to view available wireless networks. Next, I would run the Airdump-ng program to list all the Wi-Fi networks in range of my wireless card.

Let's assume the target wireless router is using WPA2. Once the target is connected the MAC address and AP will be available for viewing. I will then use Wireshark to capture the wireless network packets. Once Wireshark starts capturing packets the Wi-Fi traffic will show in the from a list.

I would then use my wireless card i to set up a fake AP using Airbase-ng. Once the AP is setup, it will show up as an available wireless network. Once someone connects it will show up on my AP in Kali Linux.

**DNS server**

I would then use DNS spoofing to trick the user into thinking they are visitng legit websites.

I would do this by “modifying the DNS records into the DNS resolver so that the query returns a malicious site”.

**Web Browser**

I would use Burp suite to execute attacks against the web browser and applications. By using a Burp suite as a proxy, I will be able to capture requests and responses between the client and the server. This will allow me to intercept the data that’s being transmitted. I will also be able to change any information about the requests before it reaches the server.

**Cloud/Virtualization**

Session riding would be the attack that I would use against the virtualization environment.

Session riding also known as a Cross Site Request forging attack is an attack that is used to replicate request on behalf of users. It gives me the ability to fake transactions and modify user information.

**Additionally, identify potential high value targets (job role only) you'd pursue**

High value targets that I would pursue would be managers, executive assistants, help desk, and system administrators. I would also target Human Resources and any new employees.

**Identify how you'd exfiltrate data without setting off network alarms.**

I would use a root kit to avoid setting off network alarms. Root kits are usually downloaded after the system has been exploited. They are used to hide files and programs. An example of a root kit is a program called Hacker Defender.For this post exploitation I would chose Hacker defender. Hack defender is a type of root kit that’s is very user friendly. It’s an easy to use to tool for beginner pen testers. It strictly for a windows environment which will be great for most tests.