CPTC Week 5 - Windows

Lab

Clone this week's Linux Pod through kamino.

- Kali credentials are `kali : kali`
- Bloodhound credentials are `admin : Qwertyuiop1!`
- Assumed Breached: `aran : WinterIsComing1`

Your target is `192.168.1.0/24`

- The router (192.168.1.1) is out of scope for this environment.

Environment

There are vulnerabilities that were not discussed or mentioned within the presentation. These vulnerabilities will give **bonus points** (max of +30). If you think you found something or need a hint, DM **@Tired Person**.

Henesys - Domain Controller
Leafre - Certificate Authority
Ariant - File Server

Deliverables

Find and exploit at least **4** vulnerabilities, and submit a formal report.

Some examples below:

- Kerberoasting
- Pass the Hash
- Credential Dumping
- ACL Abuse
- ADCS Abuses **

Within the report, explain the following:

1. Explain the vulnerability to a **technical** audience:
    a. The requirements for the vulnerability to appear (Ex. Because of A and B conditions, C becomes vulnerable to D exploit).

    b. What an attacker gains upon successful exploitation and why this is impactful.
2. Include the steps taken to **enumerate** and **exploit** the vulnerabilities.
    a. Include **screenshots** for as many steps as possible, and **explain** the commands being used.
3. How would you remediate the vulnerability?