DTU

Network Security Lab: Authentication

Zerologon

Preparation

1. It may be good to form groups for this lab! (3-5 people?)
2. If you have not setup the lab yet, go to the next slide now and follow the first 2 steps (and come back here)
3. Check out the white paper describing what is ZeroLogon.
4. Discuss the issue of this vulnerability
   a. What went wrong?
   b. What can an attacker do once it exploits this vulnerability?
   c. Can you come with some ideas about how to mitigate this issue?
5. Check out the `zerologon_tester` script. Try to understand what it does before running it.
6. Attack the Domain Controller (DC) running the tester against it.

The victim: setting a domain controller

1. Clone this repository in your computer:
   `git clone https://github.com/RicYaben/CVE-2020-1472-LAB`

2. Navigate to the clone and type `vagrant up` (this will download the VM and start it)
   a. If you are using **vmware Fusion**, go to the `Vagrantfile` and change `:vmware_desktop` for `:vmware_fusion`

3. Follow this visual tutorial to configure your VM into a Domain Controller
4. Copy the `zerologon_tester` script into your attacker VM (Kali). You will test the vulnerability from there.

Note: Do NOT run updates on the Virtual Machine! you will patch it :P
Note 2: The VM weights around 6GB, you may want to check the paper while it downloads.
Note 3: Your firewall may complain when about the tester script and the machine you are downloading. You may want to disable it (remember to re-enable it later).