Driver

Foothold

Port 80 requires authentication
-> admin:admin works!

The website allows us to upload “firmware” to the system file share

---

We can upload a malicious scf file which requests a file via smb from our box. By doing so, the user authenticates and we are able to get their NTLM hash. We can crack this NTLM hash locally.

tony:liltony

Reference:
https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/

Priv esc

The powershell history file shows a command creating a printer with a specific driver. With some research, we find that this driver can be exploited for a priv esc

https://www.pentagrid.ch/en/blog/local-privilege-escalation-in-ricoh-printer-drivers-for-windows-cve-2019-19363/
https://www.rapid7.com/db/modules/exploit/windows/local/ricoh_driver_privesc/

Using metasploit, we can get root!