Engenharia Reversa em Firmware de Roteador

Disciplina: Interface Hardware/Software

Alunos:

Filipe Nascimento Almeida

Wendel Lima Oliveira

Motivação

- Modificar o firmware do roteador para adicionar novas funcionalidades.
- Alterar a aparência da página web do roteador.

Passo 1:

- Pesquisas:

  Foram realizadas algumas pesquisas sobre o assunto e como resultado encontramos software para engenharia reversa em firmware, como:
  -- Binwalk (software para extração de imagens firmware de roteador);
  -- Firmware Analysis Toolkit (ferramenta para emulador o firmware do roteador usando o QEMU);

- Emular firmware do roteador usando o QEMU:

  Através da ferramenta FAT foi emulado o firmware de um roteador

Passo 2:

- Modificar o firmware do roteador (teste):

  -- Obtendo sucesso no passo 1 modificaremos de alguma forma (trocar uma imagem da página web ou alguma string) o firmware do roteador.

- Carregar o firmware no roteador emulado:

  -- Pós modificação do firmware do roteador voltar a implantar o firmware no roteador e testar as mudanças.

Passo 3:

- Modificação avançada:
  -- Obtendo sucesso no passo 2 elaboraríamos modificações um pouco mais complexas, como:
    --- Mudar o estilo da página web;
    --- Adicionar funcionalidade simples;

Conclusão

Pensamos em um modelo de projeto incremental que ao concluirmos uma etapa evoluiríamos para a próxima.
Esses três primeiros passos nos darão uma visão do quão complexa a nossa proposta possa ser, além de nos mostrar o conhecimento necessário para execução do projeto.