Exercise 1: Attack One Device

Phil Maker

EDS

August 2020

Abstract

A small exercise in attacking industrial control systems.

Introduction

We can vary which parts of these tasks are done (or in teams) or ... but:

- Server Target - a small server on the internet in order to extract two research papers. This is basically a recon task. Required Tools: Kali.
- Little Moata - an interface to a small nuclear reactor. Required tools: ifconfig, nmap, nc, possibly Kali along with the target machine.

To be completed over the next 7 days. You'll each get access to the reactor for 60 minutes. Note: the moata problem is designed as an exercise so don't share information till next week please and we will discuss it then.

Server Overview

A real server on the internet includes a site for you to analyse. You will need nc, nmap and Kali for this task.

- Situation: Not Such an Agency is interested in research papers on Uranium and Networking from the AAEC.
- Limitations: access only via the internet, no service attacks or intentional data destruction. No attacks via my laptop. Limit bandwidth usage to something reasonable please.
- Mission: produce a initial survelliance report for https://eds.power.on.net/cdu-target with a username of student-cdu-target using a password ??gHorseElephantHappy and ?? is a two character string.
- The next two slides identify the critical information requirements. What do you think these should be.

Server target: execution/questions

1. Whats the IP address?
2. Who is the network (Telstra?) supplier?
3. What is the router/firewall?
4. What is the target O/S, version.
5. What sort of OS (Windoze?)/http server (apache?)/application (PHP?) is it running?
6. Are there any services running port 50000-51000?
7. What do those services do if they are present?
8. Is it running PHP or ....?
9. Where is it located?

Server target: execution/questions

1. Who owns it or uses it?
2. What is the name of their first born?
3. Are there any sites on the same server?
4. Can you write a page on the wiki?
5. Can you access the files on the server, we are particularly interested in papers on Uranium Processing and Computer Networks?
6. Describe the methods you would use for a physical attack in order to retrieve the data as a short list, perhaps half a page.

Little moata

A very small nuclear reactor emulator has been implemented on the Raspberry PI (around 300SLOC). You will need nc, nmap and the ability to set up an ethernet connection for this task along with the reactor.

- Situation: We have obtained access to the ethernet port on a small nuclear reactor (PI : SL-2). Access is via the ethernet port its address is somewhere in the 10.200.0.0/24 range. The controller is believed to have its own custom TCP based protocol but we do not have access to a specification at ths time.
- Limitations: no access via HMDI video, wifi, ... or hardware. Just us the ethernet port.
- Mission: analyse and possibly destroy the target.

Litte Moata: execution

- Execution: the mission is to conducted in three parts.
  - Find: submit a written description of the system and its protocols based on active testing. Report must include:
    - Port numbers, IP addresses, O/S (OpenBSD?),...
    - Protocol conventions as they appear to you for the port in the 50000..60000 range. Any other open ports.
    - Accessible variables and give your interpretation of their possible meanings.
  - Fix: confirm that you can change variables via the protocol using non critical values. Then submit a written plan for the destruction of the asset for approval by No Such Agency.
  - Finish: execute the plan resulting in one or more of:
    - Force a variable via the protocol
    - Change Power Output of the system
    - Disable the emergency generators.
    - Scram!!!! message on the port, and it will recover in 60s
    - Meltdown!!!! message on the port, and it won't recover.

  Write up a single page report on the results, including any scripts you have used.

Conclusion

In this exercise it is intended that you have:

- Used port mapping, etc to conduct a basic survelliance task on a single target.
- Analysed a simple industrial protocol along with a modelled physical system in order to conduct an attack.

The next exercise will be a defence of the many, in contrast to an attack on the few. Thanks.