OTW Jan 2 4 min read

SCADA Hacking: Hacking the Schneider Automated Building System

SCADA and ICS systems control industrial processes around the world. Everything from railroads, to traffic lights, to oil refineries to commercial buildings are all

controlled by these SCADA/ICS systems. Some of the recent concern about these

systems is the possible hacking of them by terrorists or by cyber war opponents. In either case, the results could be devastating (the Bhopal disaster at the Union Carbide plant cost over 30,000 lives). Despite this, these systems are unusually vulnerable to hacking and malicious activity.

In this tutorial, I will show how to hack into an industrial control system manufactured by Schneider Electric, one of the world's largest manufacturers of SCADA/ICS systems. Due to lax embedded security at development, some of these systems are incredibly easy to hack into and take control of the building.

Schneider Electric Building Automation Servers

Schneider Electric is a Paris-based company, well-known in the Industrial control industry. In fact, they are a pioneer in this field, having developed the most widely used protocol used in industrial control systems, modbus.

Schneider Electric makes products that use digital controls in industrial applications. This digital controllers are Programmable Logic Controllers or PLC's. They use these

PLC's in many different industrial applications including building automation

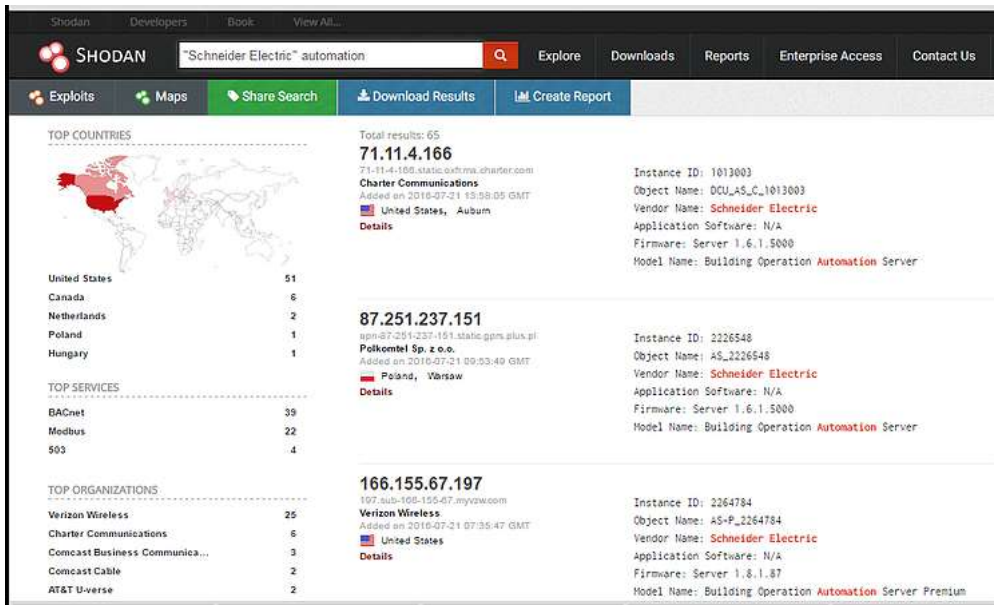
products and sell them throughout the world.

One of their products, Schneider-Electric Automation Server, is used in commercial buildings to control and automate their many systems including heating and cooling, lighting, security, etc.

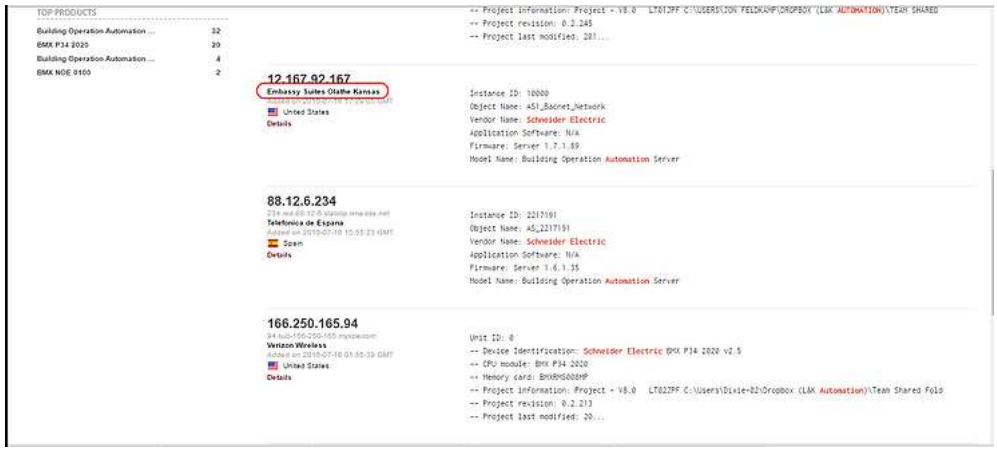
Finding the Schneider Automation Servers with Shodan

We can find these Automation server in Shodan by searching for "Schneider-Electric" automation.

"Schneider Electric" automation



If we scroll down a bit through this list, we can see a major hotel on Kansas City using these automation servers, among many others.



A few months back, an independent security researcher, Karn Ganeshen, found a major vulnerability in these automation servers that allows nearly anyone to take control of them. Let's try that. I'll be using Kali Linux, but since this hack is so simple, just about any Linux will do.

The Vulnerability

This vulnerability enables the attacker to connect to the Automation Server with SSH

using default credentials and then escalate their privileges to "root". Once the attacker has root privileges, they not only own the box, but the entire building!

Connecting to the Building Automation Server

First, let's find a Schneider Electric Automation Server and connect to it with SSH. The command is simple.

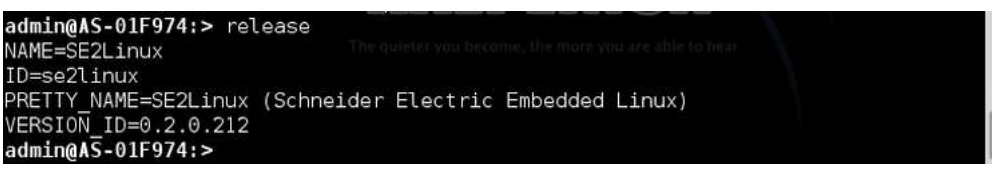
kali > ssh <IP> -l admin

After we have connected, the server will prompt us for a password. Use the default password "admin".

You will then be greeted by the Automation Server's admin account .

We can type "help" to see what commands we can use from this account.

For instance, let's type "release". As you can see below, the system responds with the version information of the server. Also, note that one of the commands is "reboot", which may be useful in a DoS attack against this system.



We can also see the time since the last reboot, by typing "uptime".

admin > uptime

This type of information is always useful to an attacker as it indicates, usually, the last time the system was patched.

One of the many weaknesses of this system is that we can **pipe system commands to the underlying server** after these SSH commands. So, for instance, we can see the passwd file on the underlying server by typing;

admin> uptime | cat /etc/passwd

As you can see, we now have listed all the accounts on this server. Of course, this file only contains the accounts and not the passwords. Passwords are in the /etc/shadow file and only root has access to that file.

Getting Root

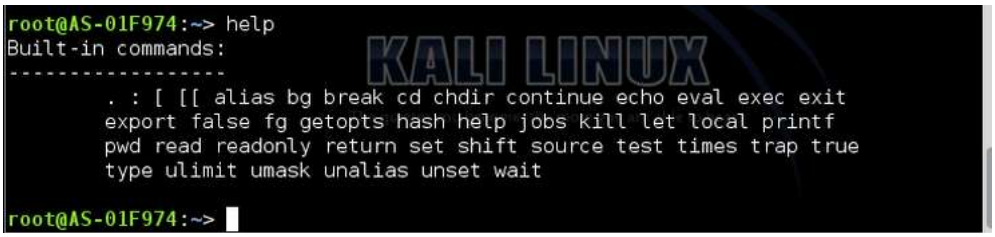
Of course, to own this server we will want root privileges. We can escalate our privileges by simply typing;

admin > sudo -i

The default configuration of this building automation server has no password for the "root" account, so simply hit **Enter** when prompted for a password.

As you can see, the prompt turns green and indicates that **we are root!**

Now, let's type "help" here to see what commands are available to us on this account.



Since we now have root privileges on this box, we should be able to do just about anything! Let's see whether we can pull up the password hashes at /etc/shadow.

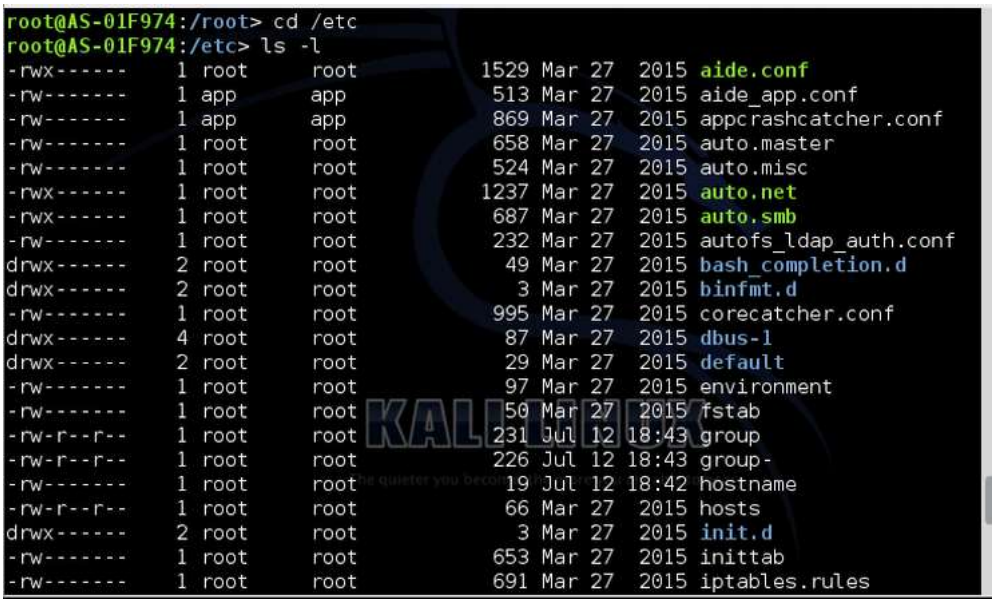
AS > cat /etc/shadow

As you can see, we were able to get all the accounts and their password hashes! If needed, we could run these hashed passwords through a brute force cracker like hashcat to retrieve the plaintext passwords.

It's likely that the configuration file for the Automation Server is in the /etc directory. Let's go there and list all the files and directories.

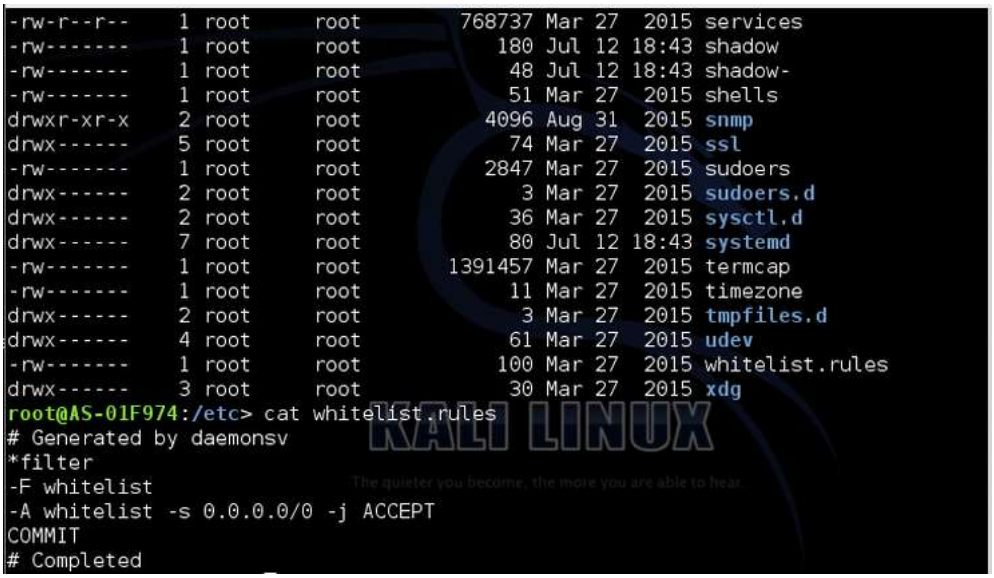
AS> cd /etc

AS > ls -l



If we scroll down this list a bit, we will see a files called "whitelist.rules". This is a file to determine who can connect to this server. Let's open it.

AS > cat whitelist.rules



As you can see, the system admin had never setup the whitelist.rules on this server and as a result, anyone can connect.

Finally, since we have root privileges, we can add new users. Before I leave, I can add myself to the users, give myself root privileges, and add myself to the whitelist.rules, so that even if the admin remediates this vulnerability, I will still have an account and be able to access this server.

I hope it goes without saying that now that I have access to the system with root privileges, I can change and manipulate this system anyway I want!

I hope this highlights how vulnerable these systems are and what a rich field SCADA/ICS hacking is!

Recent Posts See All

Automobile Hacking, Part 2: The can-utils or SocketCAN

9,940 Write a comment 1

OSINT, Part 6: Open-Source Flight and Aircraft Tracking Data

602 Write a comment

Open Source Intelligence (OSINT): Reverse Image Searches for Investigat...

353 Write a comment

Log in to leave a comment.