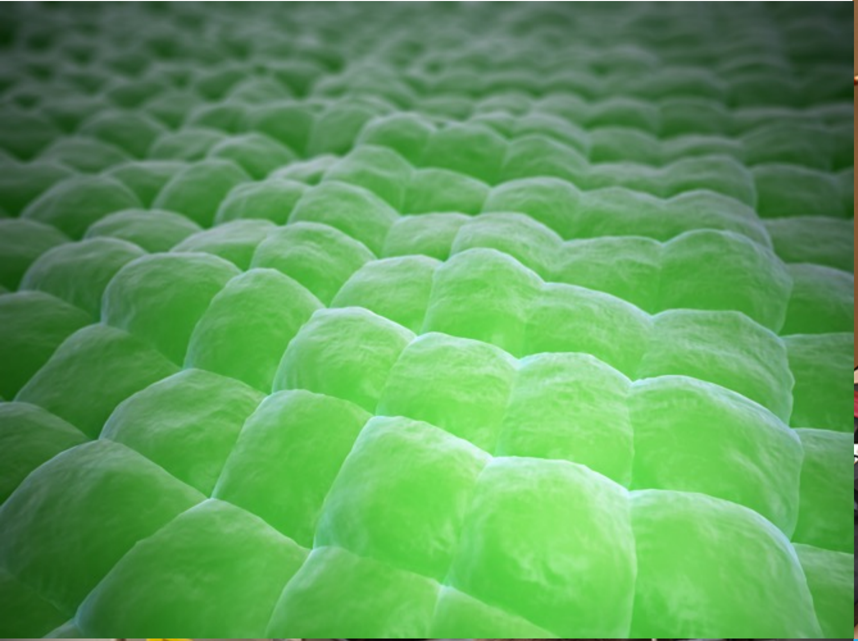


INL/CON-23-74522

September 14, 2023

**Megan Culler**
INL Power Engineer

# CyberStrike STORMCLOUD

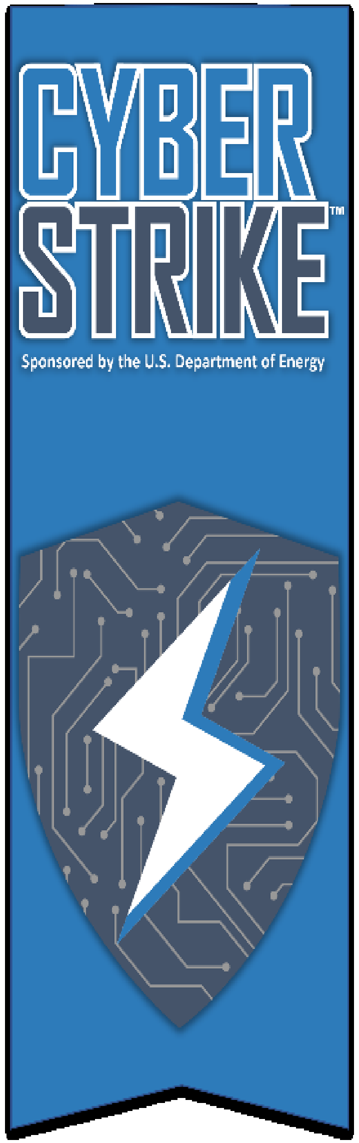
INL & Sandia

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

INL Idaho National Laboratory

# What is CyberStrike?

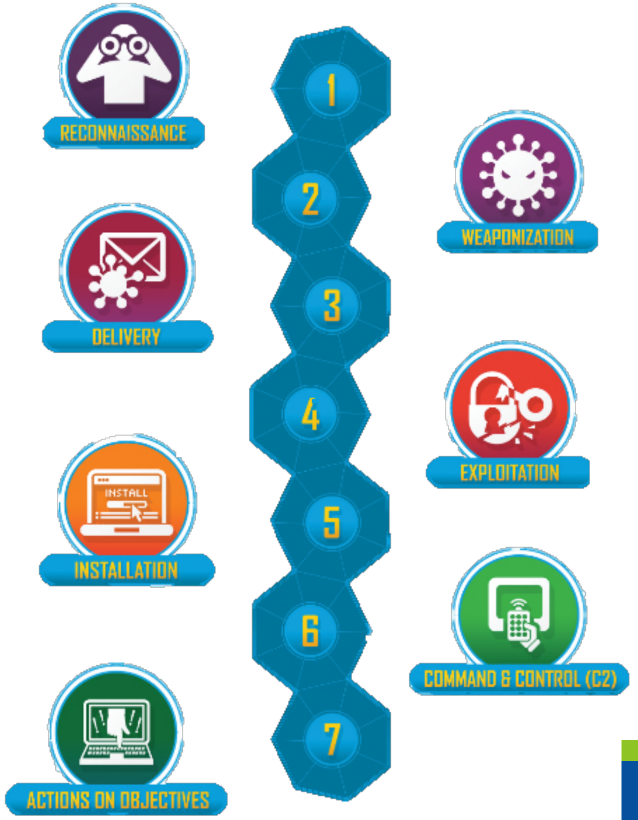
CyberStrike is a training program designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting operational technology .



# What is CyberStrike STORMCLOUD?

The *CyberStrike STORM CLOUD training workshop was designed to enhance the ability of renewable energy and operators to prepare for a cyber incident impacting industrial control systems with specific considerations of the architectures and limitations of renewable energy.*

- Renewables focused
  - Solar
  - Wind (coming soon)
  - EVs (coming soon)
- Emphasis on emerging and unique threats for renewables
  - Remote access
  - Diverse stakeholder ecosystem
- Framework uses Lockheed Cyber Kill Chain



U.S. DEPARTMENT OF ENERGY

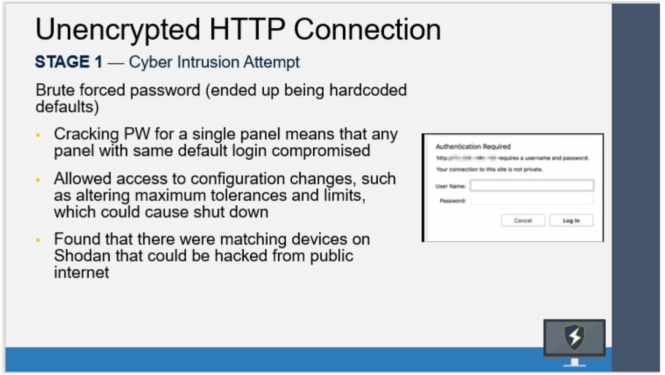
Energy Efficiency & Renewable Energy

U.S. DEPARTMENT OF ENERGY

Office of Cybersecurity, Energy Security, and Emergency Response

# CyberStrike STORMCLOUD

## Curriculum



### Unencrypted HTTP Connection

**STAGE 1** — Cyber Intrusion Attempt

Brute forced password (ended up being hardcoded defaults)

- Cracking PW for a single panel means that any panel with same default login compromised
- Allowed access to configuration changes, such as altering maximum tolerances and limits, which could cause shut down
- Found that there were matching devices on Shodan that could be hacked from public internet

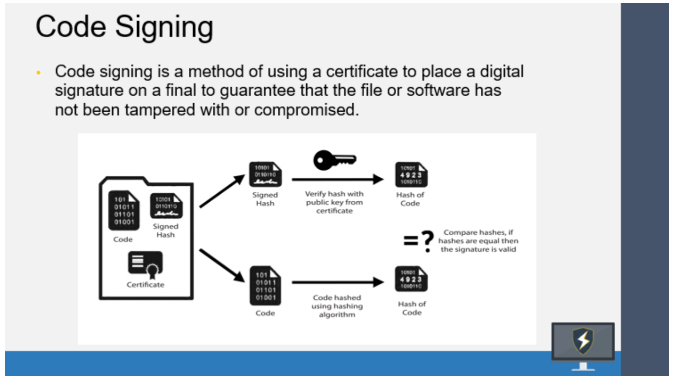
Authentication Required

http://[redacted] requires a username and password.

Your connection to this site is not private.

User Name:

Password:

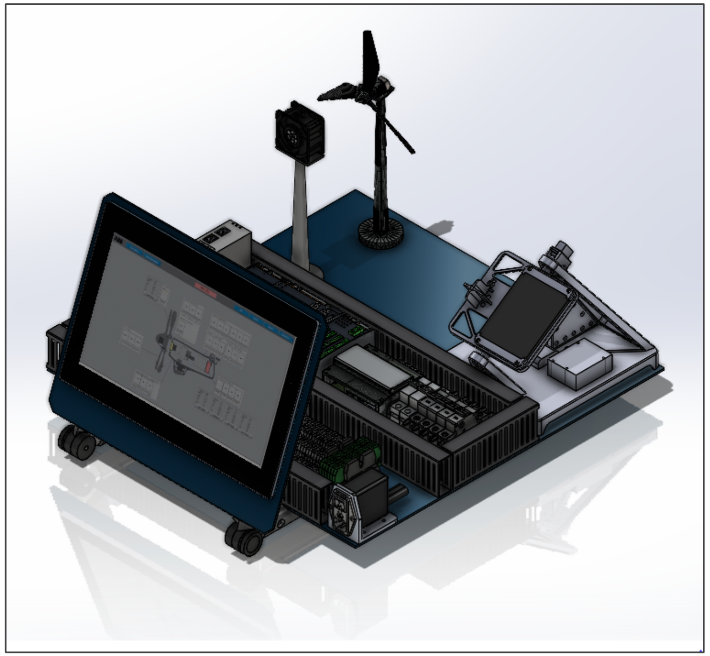


### Code Signing

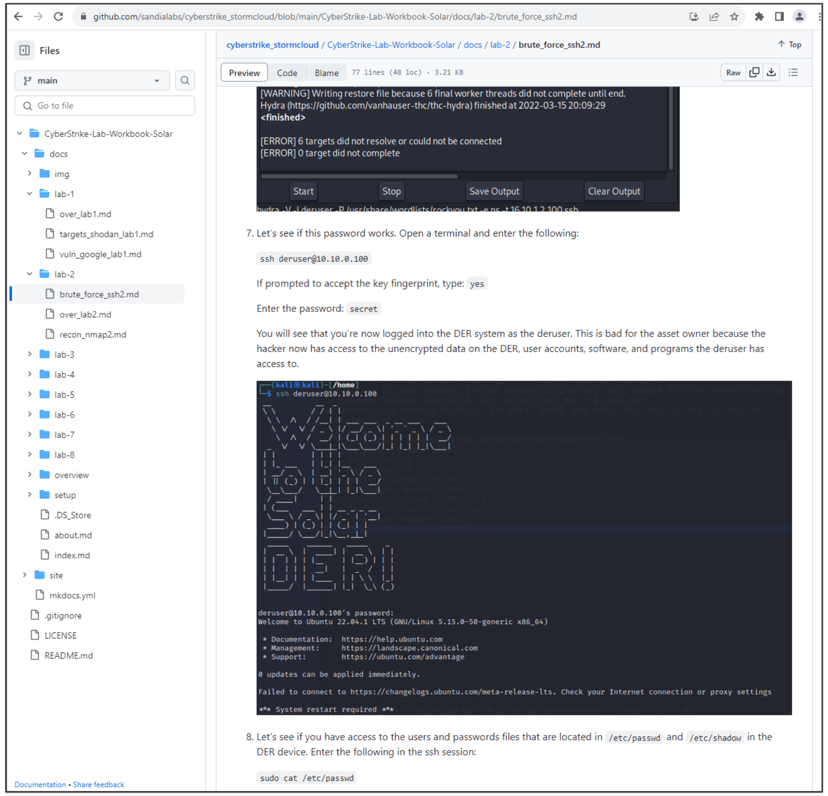
- Code signing is a method of using a certificate to place a digital signature on a final to guarantee that the file or software has not been tampered with or compromised.

Code
Signed Hash
Certificate
Signed Hash
Verify hash with public key from certificate
Hash of Code
=?
Compare hashes, if hashes are equal then the signature is valid
Code
Code hashed using hashing algorithm
Hash of Code

## Hardware



## Exercises



github.com/sandialabs/cyberstrike_stormcloud/blob/main/CyberStrike-Lab-Workbook-Solar/docs/lab-2/brute_force_ssh2.md

```
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-15 20:09:29
<finished>

[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
```

```
hydra -V -l deruser -P /usr/share/wordlists/rockyou.txt -e ns -t 16 10.1.2.100 ssh
```

7. Let's see if this password works. Open a terminal and enter the following:

   `ssh deruser@10.10.0.100`

   If prompted to accept the key fingerprint, type: `yes`

   Enter the password: `secret`

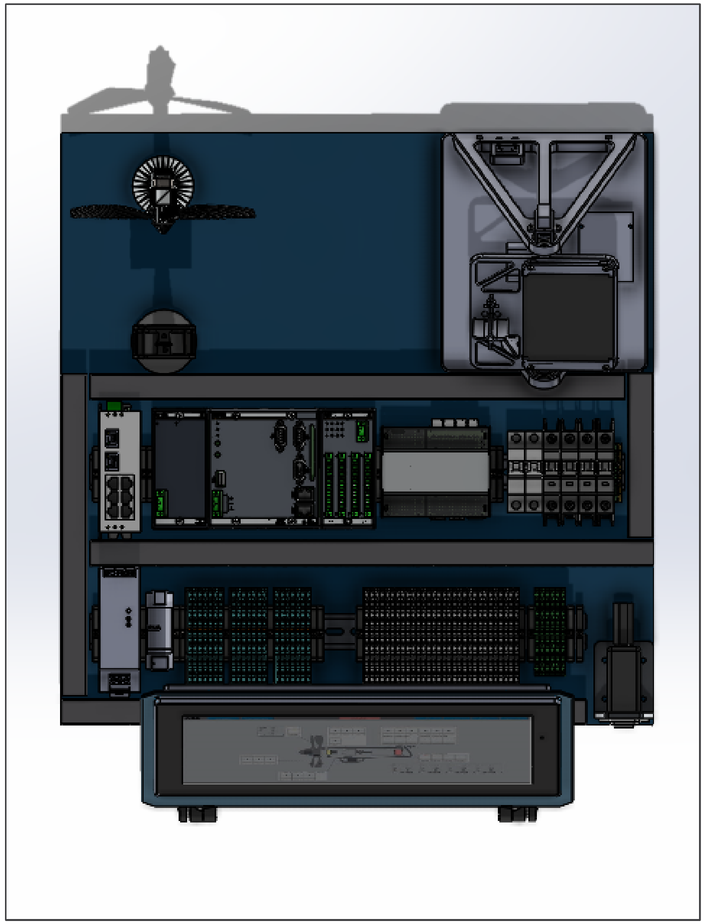
   You will see that you're now logged into the DER system as the deruser. This is bad for the asset owner because the hacker now has access to the unencrypted data on the DER, user accounts, software, and programs the deruser has access to.

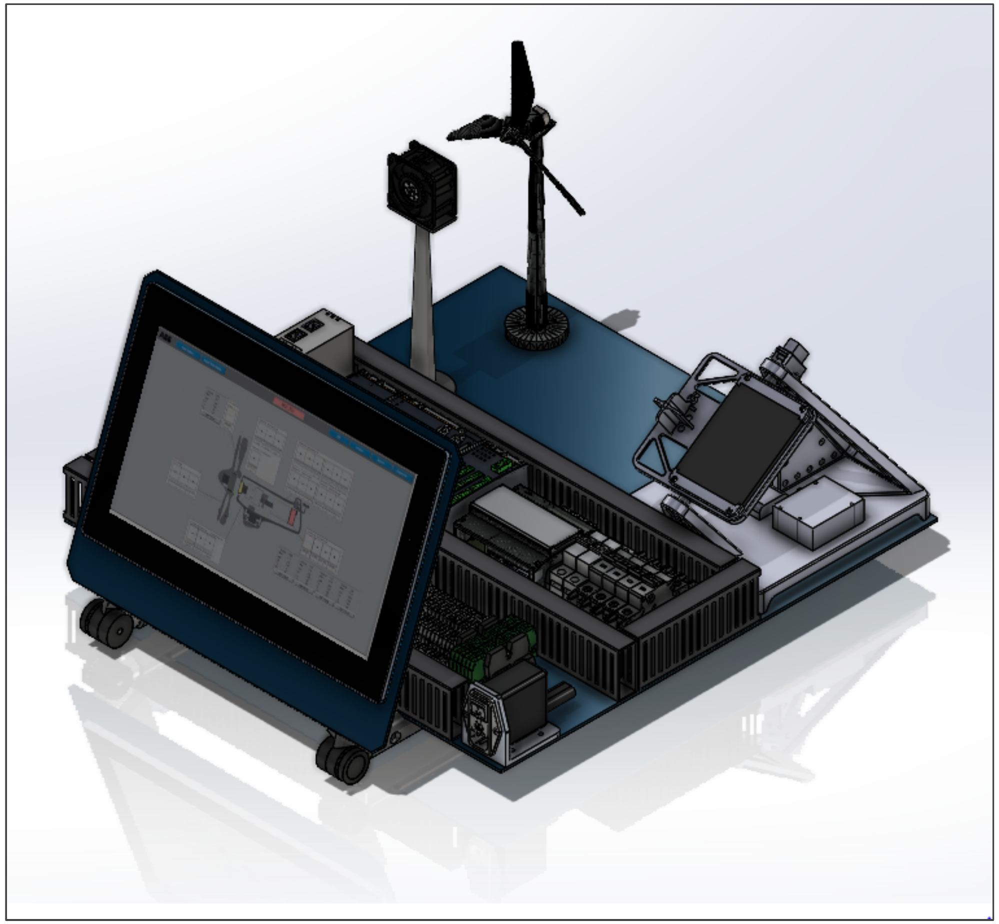
```
┌──(kali㉿kali)-[/home]
└─$ ssh deruser@10.10.0.100

deruser@10.10.0.100's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***
```

8. Let's see if you have access to the users and passwords files that are located in `/etc/passwd` and `/etc/shadow` in the DER device. Enter the following in the ssh session:

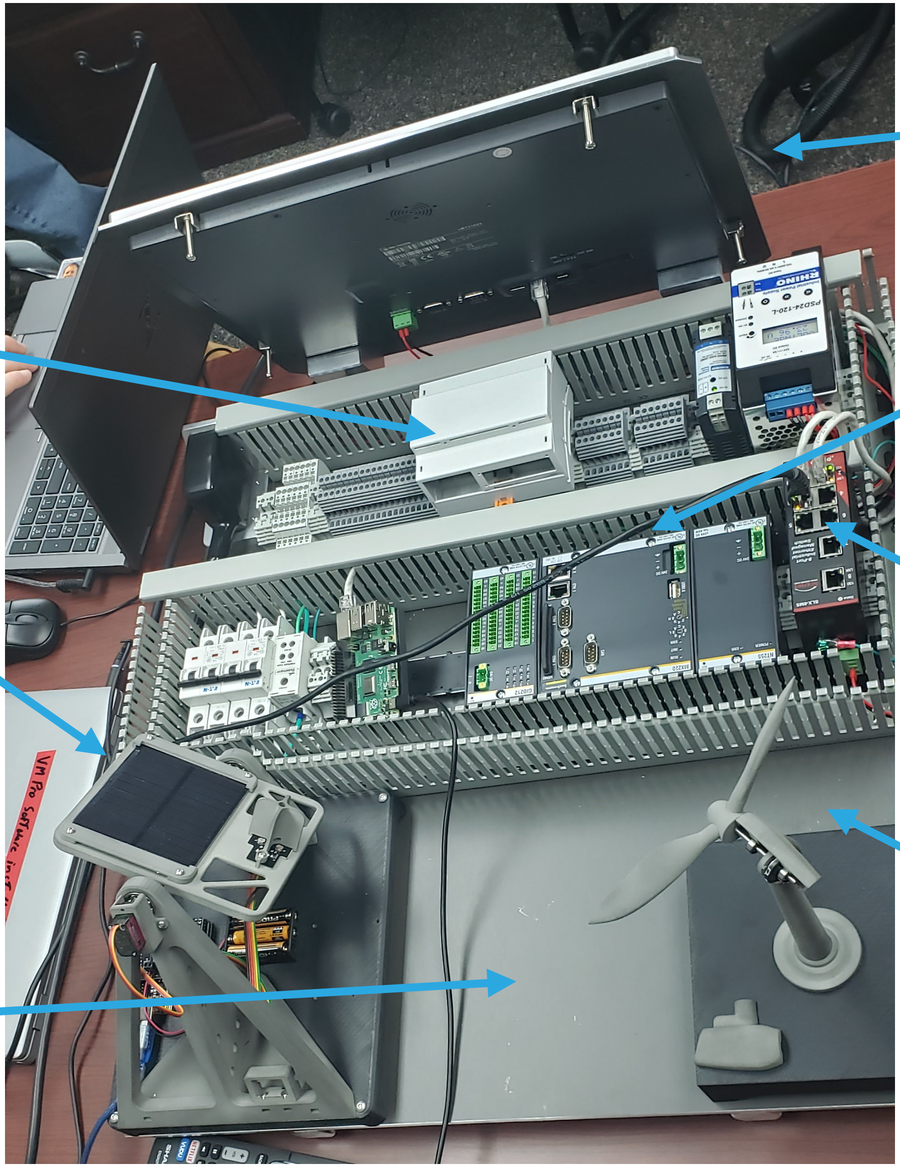
   `sudo cat /etc/passwd`

# STORMCLOUD Kit Design





# CyberStrike Storm Cloud Demo Kit



HMI

Solar “inverter” – Raspberry Pi emulator

Industrial controller to be used for wind

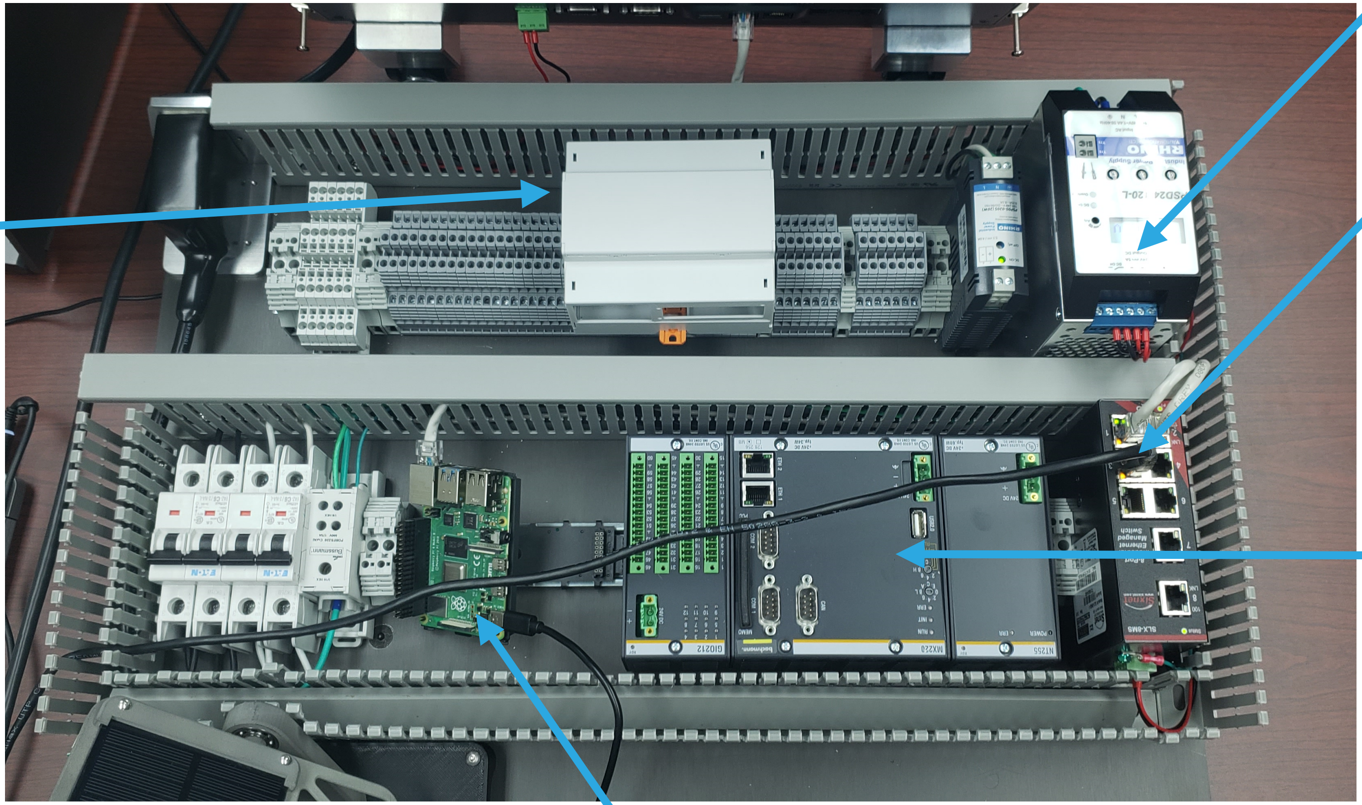
Network switch for the DER system

Single-axis solar

Open platform design to allow wind turbine to blow

Space for EV model

# CyberStrike Storm Cloud Demo Kit - Networking



Raspberry Pi inverter emulation

5 V power supply

Network switch

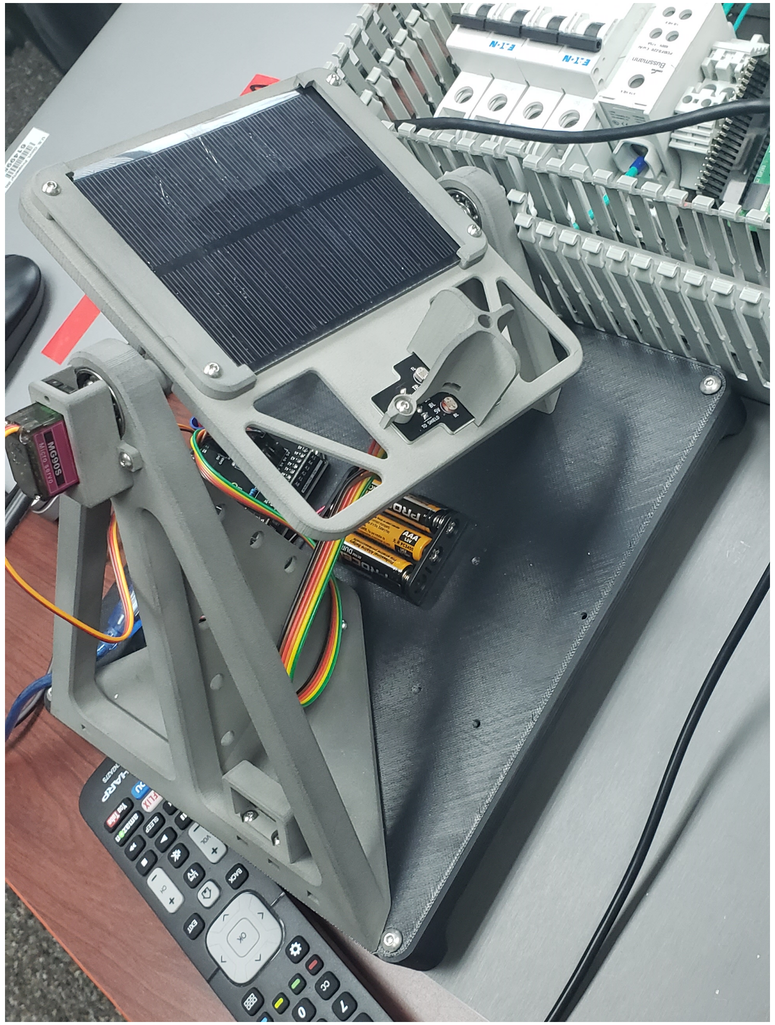
Industrial controller for wind

Arduino board governing solar tracker

# CyberStrike Storm Cloud Demo Kit – Solar module

Photoresistor measures output

3D-printed Nylon custom frame

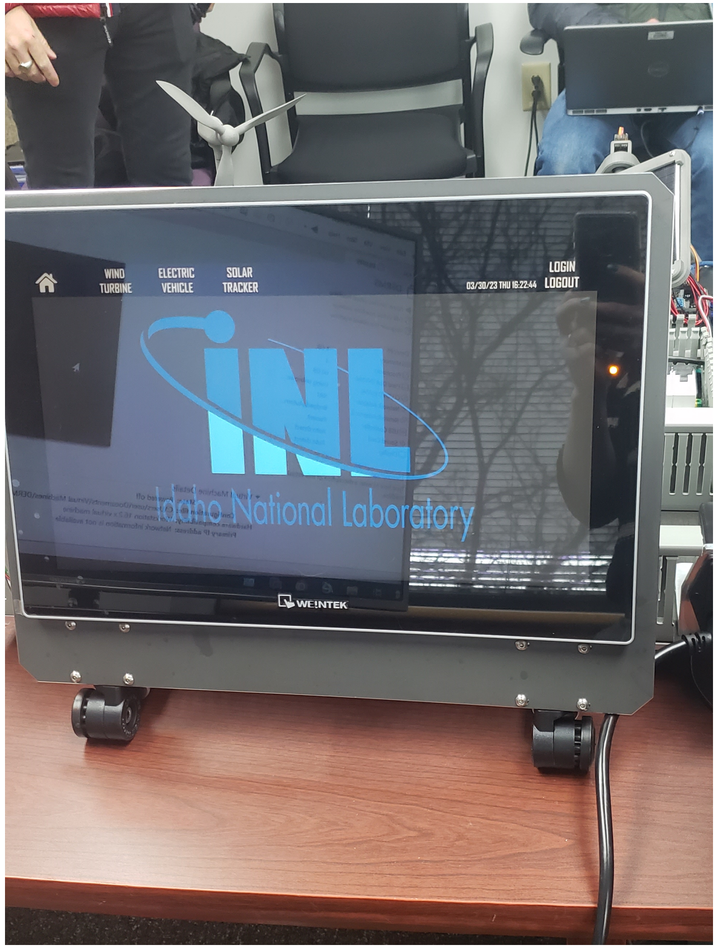


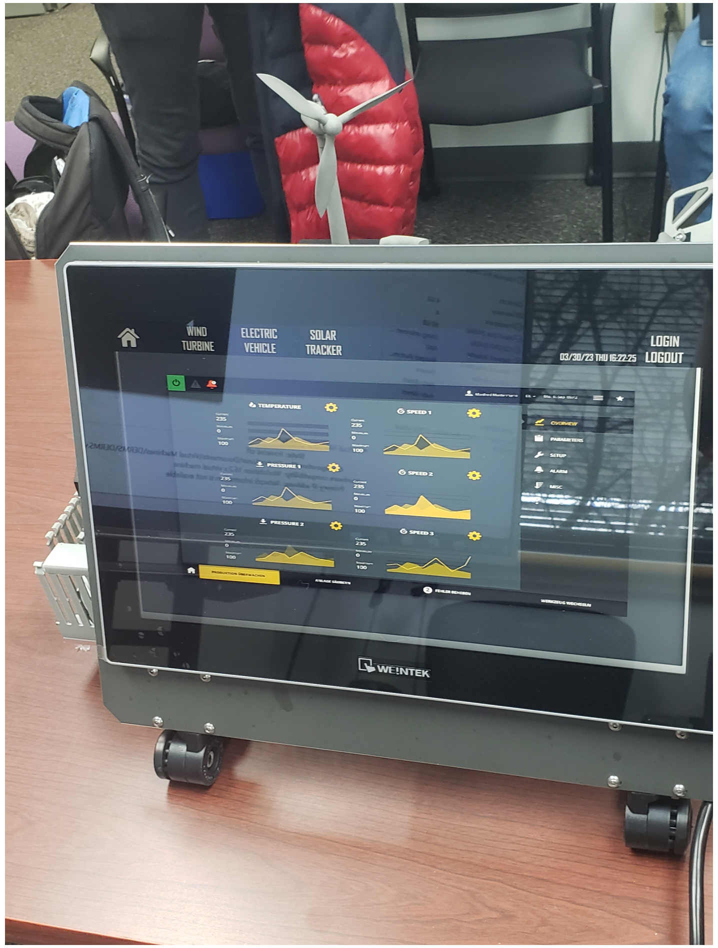
Arduino program uses photo-resistor output to determine an angle for the mount.

# CyberStrike Storm Cloud Demo Kit – HMI

Touch screen HMI

Separate tabs for each resource





Wind mockup display

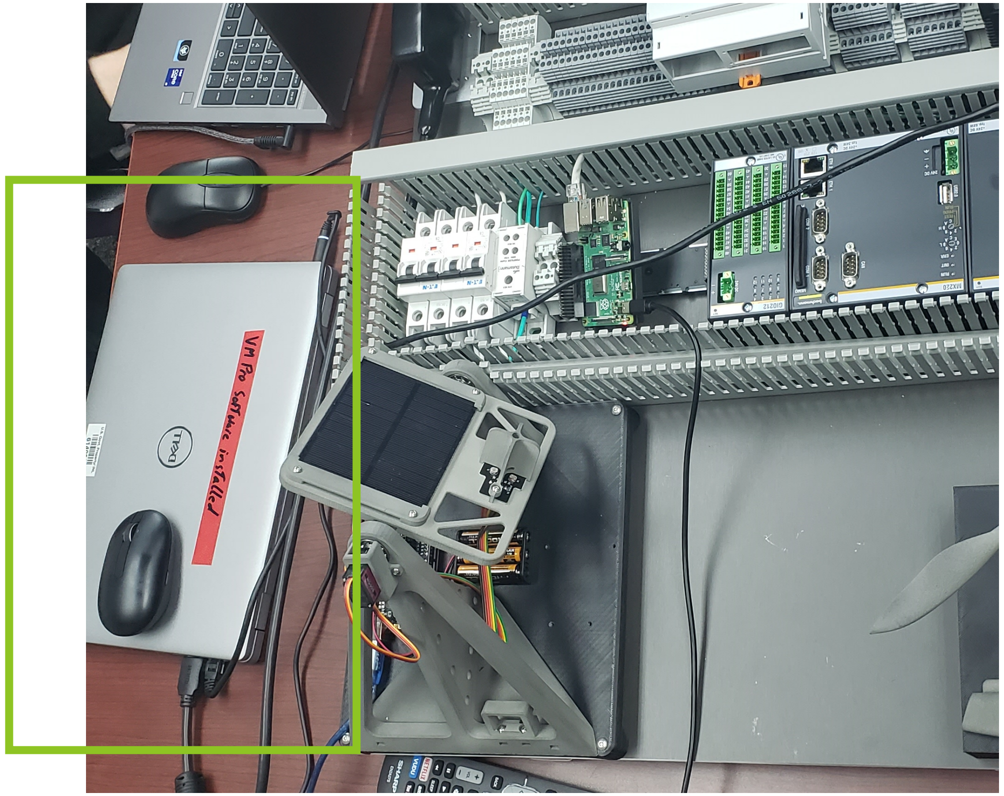
No current applications for solar (not representative of industry)

# CyberStrike Storm Cloud Demo Kit - Software

Workstation is a Kali Linux machine

Two VMs used to run the exercises

- Attacker Kali VM
- DERMS Windows VM



Lab manual on VM images for easy access

Lab exercises currently developed:

- Uses real solar firmware images
- Uses real solar protocols

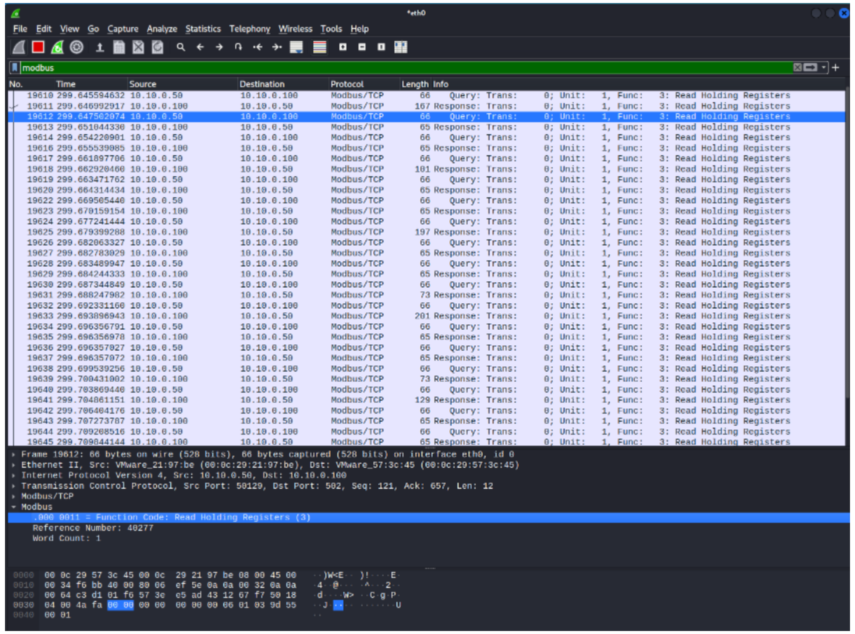
# Lab Interfaces and Tools

## Cybersecurity Tools

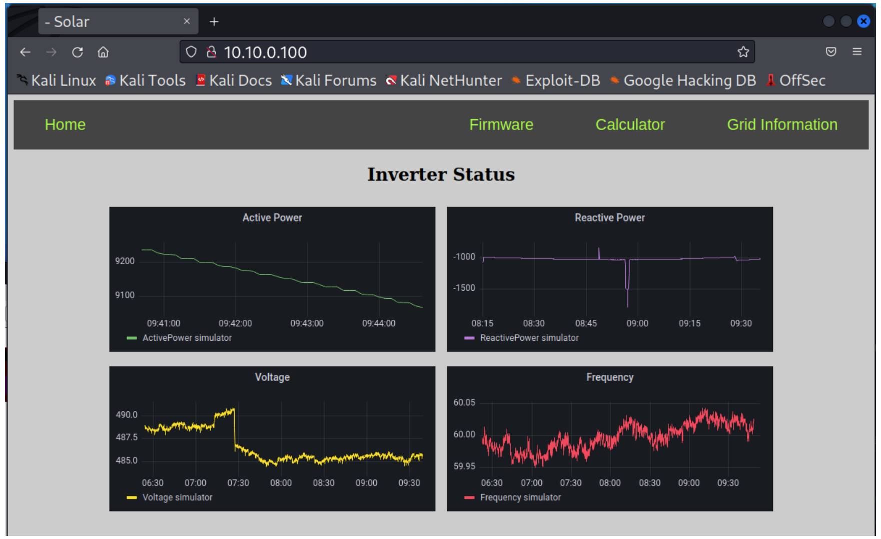
- Shodan
- Xhydra
- NMAP
- Wireshark
- Ettercap

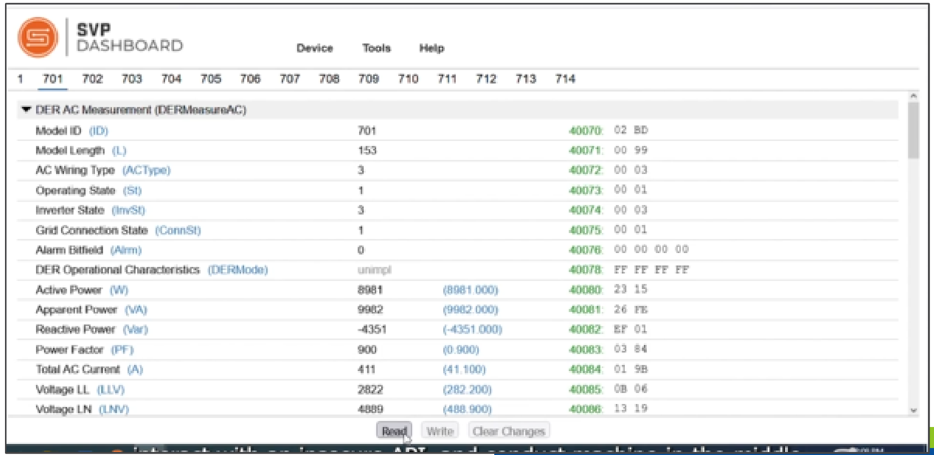
## DER Interfaces

- Custom web interface
- VNC Viewer
- SSH
- SunSpec MODBUS
- IEEE 2030.5


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
modbus

```
No.   Time          Source       Destination  Protocol   Length Info
19610 299.645594632 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19611 299.646992917 10.10.0.100  10.10.0.50   Modbus/TCP 167 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19612 299.647502074 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19613 299.651044330 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19614 299.654220901 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19616 299.655539085 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19617 299.661897706 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19618 299.662920460 10.10.0.100  10.10.0.50   Modbus/TCP 101 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19619 299.663471762 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19620 299.664314434 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19622 299.669505440 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19623 299.670159154 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19624 299.677241444 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19625 299.679399288 10.10.0.100  10.10.0.50   Modbus/TCP 197 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19626 299.682063327 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19627 299.682783029 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19628 299.683489947 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19629 299.684244333 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19630 299.687344849 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19631 299.688247982 10.10.0.100  10.10.0.50   Modbus/TCP  73 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19632 299.692331160 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19633 299.693896943 10.10.0.100  10.10.0.50   Modbus/TCP 201 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19634 299.696356791 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19635 299.696356978 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19636 299.696357027 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19637 299.696357072 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19638 299.699539256 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19639 299.700431002 10.10.0.100  10.10.0.50   Modbus/TCP  73 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19640 299.703869440 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19641 299.704861151 10.10.0.100  10.10.0.50   Modbus/TCP 129 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19642 299.706404176 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19643 299.707273787 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19644 299.709268516 10.10.0.50   10.10.0.100  Modbus/TCP  66    Query: Trans:    0; Unit:   1, Func:   3: Read Holding Registers
19645 299.709844144 10.10.0.100  10.10.0.50   Modbus/TCP  65 Response: Trans:    0; Unit:   1, Func:   3: Read Holding Registers

> Frame 19612: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_21:97:be (00:0c:29:21:97:be), Dst: VMware_57:3c:45 (00:0c:29:57:3c:45)
> Internet Protocol Version 4, Src: 10.10.0.50, Dst: 10.10.0.100
> Transmission Control Protocol, Src Port: 50129, Dst Port: 502, Seq: 121, Ack: 657, Len: 12
> Modbus/TCP
v Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    Reference Number: 40277
    Word Count: 1

0000  00 0c 29 57 3c 45 00 0c  29 21 97 be 08 00 45 00   ··)W<E·· )!····E·
0010  00 34 f6 bb 40 00 80 06  ef 5e 0a 0a 00 32 0a 0a   ·4··@··· ·^···2··
0020  00 64 c3 d1 01 f6 57 3e  e5 ad 43 12 67 f7 50 18   ·d····W> ··C·g·P·
0030  04 00 4a fa 00 00 00 00  00 00 00 06 01 03 9d 55   ··J····· ·······U
0040  00 01                                              ··
```



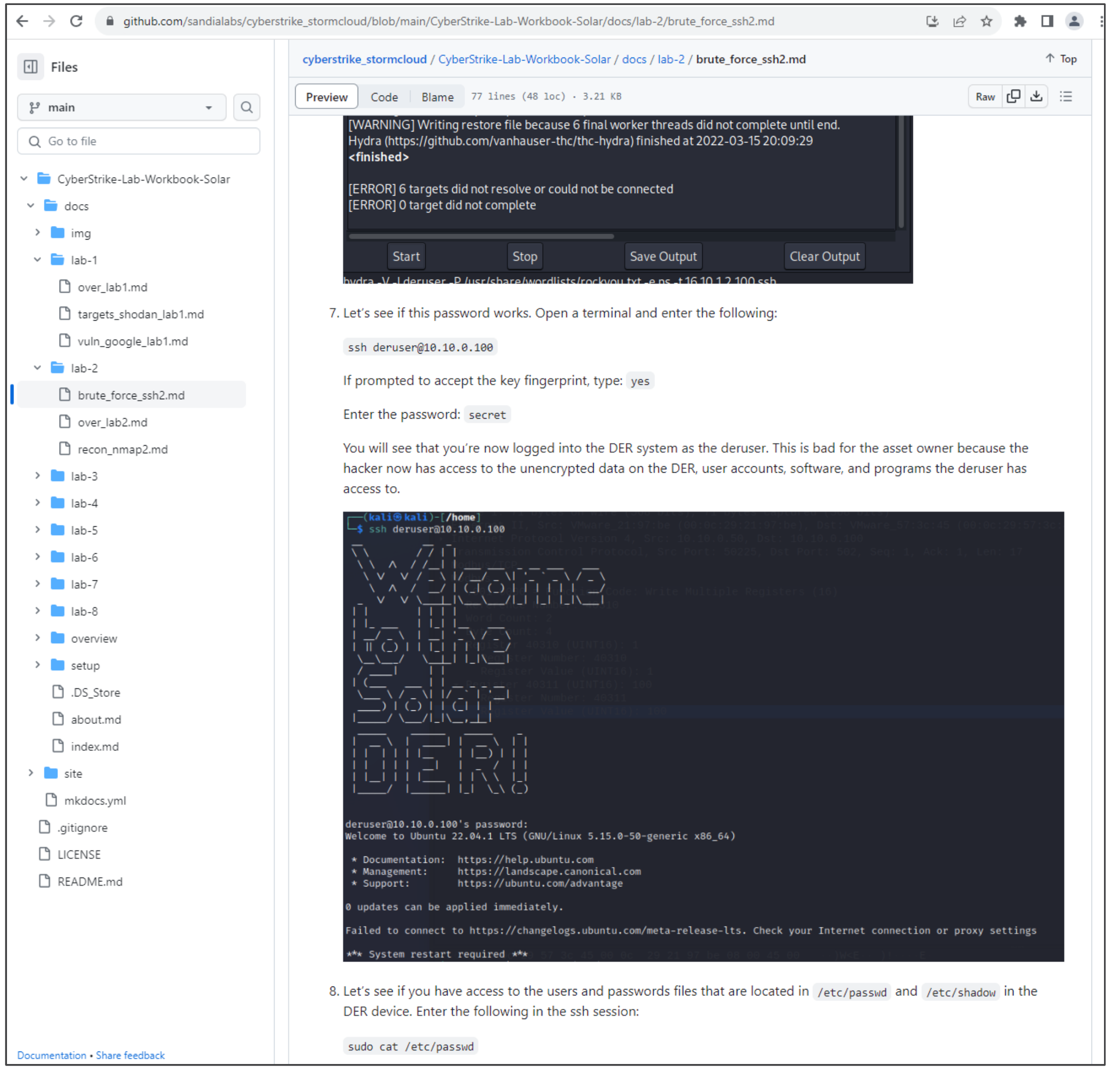


DER AC Measurement (DERMeasureAC)

| | | | | |
|---|---|---|---|---|
| Model ID (ID) | 701 | | 40070: | 02 BD |
| Model Length (L) | 153 | | 40071: | 00 99 |
| AC Wiring Type (ACType) | 3 | | 40072: | 00 03 |
| Operating State (St) | 1 | | 40073: | 00 01 |
| Inverter State (InvSt) | 3 | | 40074: | 00 03 |
| Grid Connection State (ConnSt) | 1 | | 40075: | 00 01 |
| Alarm Bitfield (Alrm) | 0 | | 40076: | 00 00 00 00 |
| DER Operational Characteristics (DERMode) | unimpl | | 40078: | FF FF FF FF |
| Active Power (W) | 8981 | (8981.000) | 40080: | 23 15 |
| Apparent Power (VA) | 9982 | (9982.000) | 40081: | 26 FE |
| Reactive Power (Var) | -4351 | (-4351.000) | 40082: | EF 01 |
| Power Factor (PF) | 900 | (0.900) | 40083: | 03 84 |
| Total AC Current (A) | 411 | (41.100) | 40084: | 01 9B |
| Voltage LL (LLV) | 2822 | (282.200) | 40085: | 0B 06 |
| Voltage LN (LNV) | 4889 | (488.900) | 40086: | 13 19 |

# Lab Exercises

- Reconnaissance
  - OSINT demo
  - NMAP port scanning
- Brute-forced passwords
  - Password cracking tools
- Denial-of-service
  - Network flooding
- Malicious firmware updates
  - Code signing and certificates
- Web exploitation
  - SQL injection
  - Code injection
- App inspection
  - Credential harvesting
- Replay and Man-in-the-middle
  - ARP spoofing and packet modification
- Defense
  - Host-based firewall rules



```
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-15 20:09:29
<finished>

[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
```

```
hydra -V -l deruser -P /usr/share/wordlists/rockyou.txt -e ns -t 16 10.1.2.100 ssh
```

7. Let's see if this password works. Open a terminal and enter the following:

   `ssh deruser@10.10.0.100`

   If prompted to accept the key fingerprint, type: `yes`

   Enter the password: `secret`

   You will see that you're now logged into the DER system as the deruser. This is bad for the asset owner because the hacker now has access to the unencrypted data on the DER, user accounts, software, and programs the deruser has access to.

```
┌──(kali㉿kali)-[/home]
└─$ ssh deruser@10.10.0.100

deruser@10.10.0.100's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***
```

8. Let's see if you have access to the users and passwords files that are located in `/etc/passwd` and `/etc/shadow` in the DER device. Enter the following in the ssh session:

   `sudo cat /etc/passwd`

https://github.com/sandialabs/cyberstrike_stormcloud/

# FY24 Plans

- Virtualization
  - Virtual platform allows students to take the training on their own time.
  - Interaction with hardware occurs through virtual machines and IP cameras watching the hardware.
- Updated curriculum with 2023 events and vulnerabilities
  - Keep content relevant
  - Update based on feedback from industry events
- Industry engagement
  - Target workshops at relevant industry events to continue rollout and solicit feedback

INL

Idaho National Laboratory

*Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.*

WWW.INL.GOV