Simulating The 2015 Ukraine Cyber Attack on Power Grid Testbed

[1]Jonathan McBride, [2]Aaron Werth, [2]Raymond Borges Hink, [2]Gary Hahn, [2]Emillo Piesciorovsky [3]Holden Goff, [4]Timothy Alhorn
[1]SANS Technology Institute, [2]Oak Ridge National Laboratory, [3]University of Alabama, [4]Tennessee Technological University

Introduction

Background: Ukraine has experienced multiple cyberattacks towards its power grid. The 2015 cyberattack highlighted the crucial significance of cybersecurity measures for critical infrastructure [1]. The impact of these attacks display the importance of cyber protection towards the United States power grid.

Aim: The goal of the attacks and study is to emulate cyberattacks that occurred towards Ukraine's power grid in recent years while recreating ICS Kill Chain attack methods used as seen in *Figure 3*.

Methodology: The cyberattacks were performed on a virtual testbed using virtual machines. Software used for this attack was Nmap which is a network host scanner, Metasploit, and Meterpreter was used to exploit security vulnerabilities.

Testbed

Testing Environment: The testbed in *Figure 1*, displays the network topology that was used to emulate the Ukraine attack. The Kali machine (node1) was used as the attacker machine to exploit vulnerabilities on all the other nodes on the virtual testbed. The testbed in *Figure 2*, is the simulated physical electrical substation-grid testbed with Distributed Ledger Technology (DLT), relays, and timing systems.

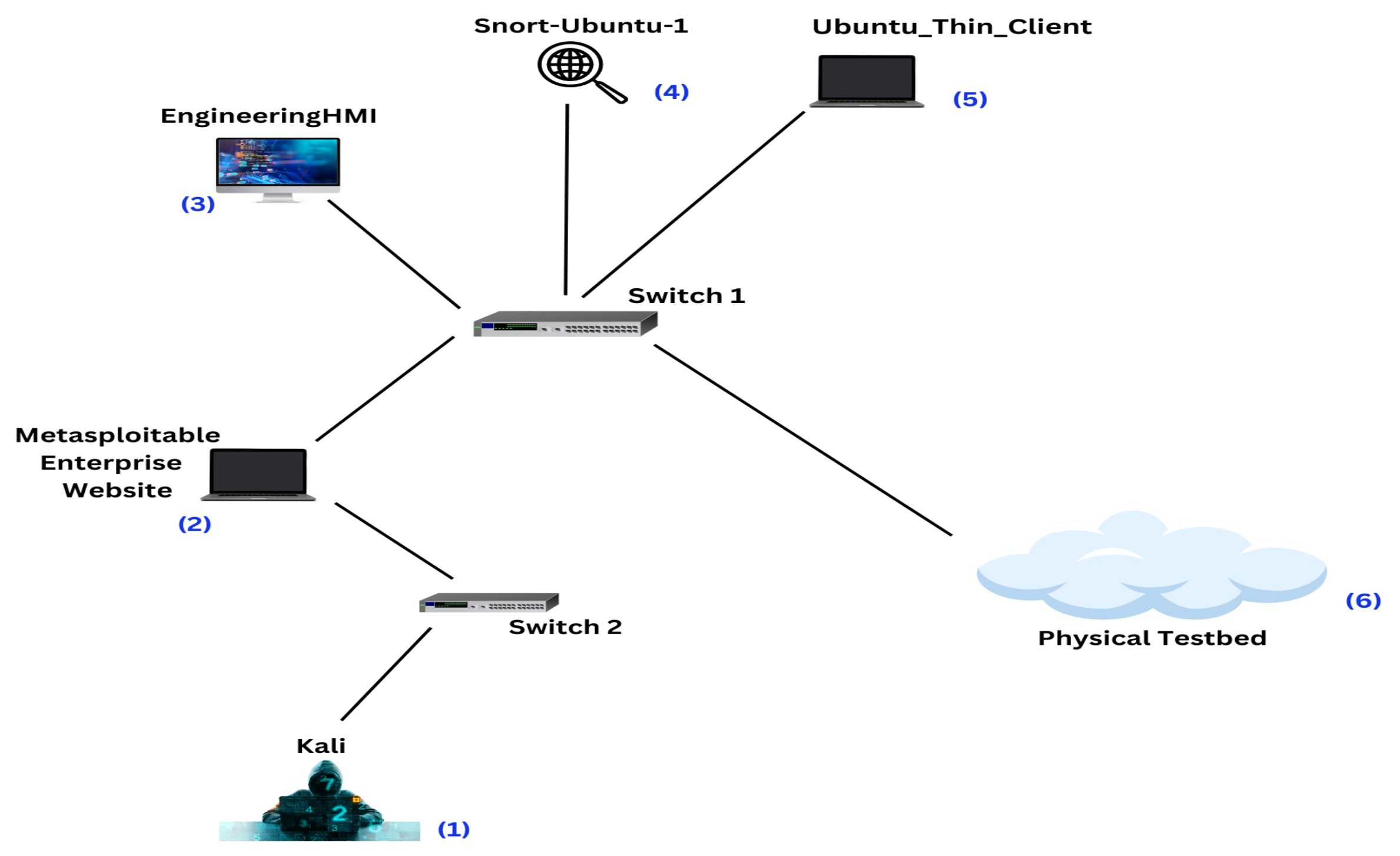


Figure 1. Virtual Testbed

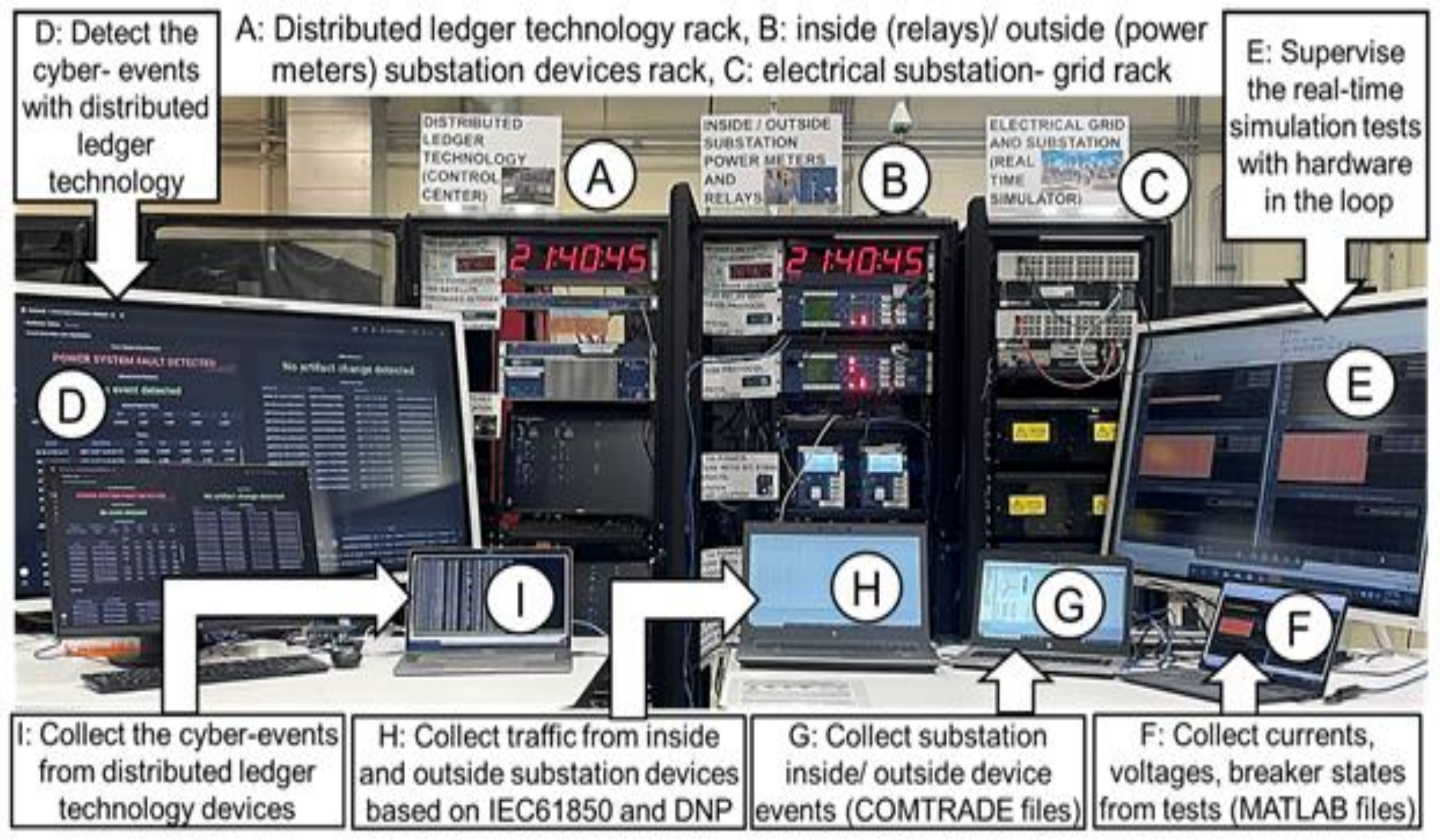
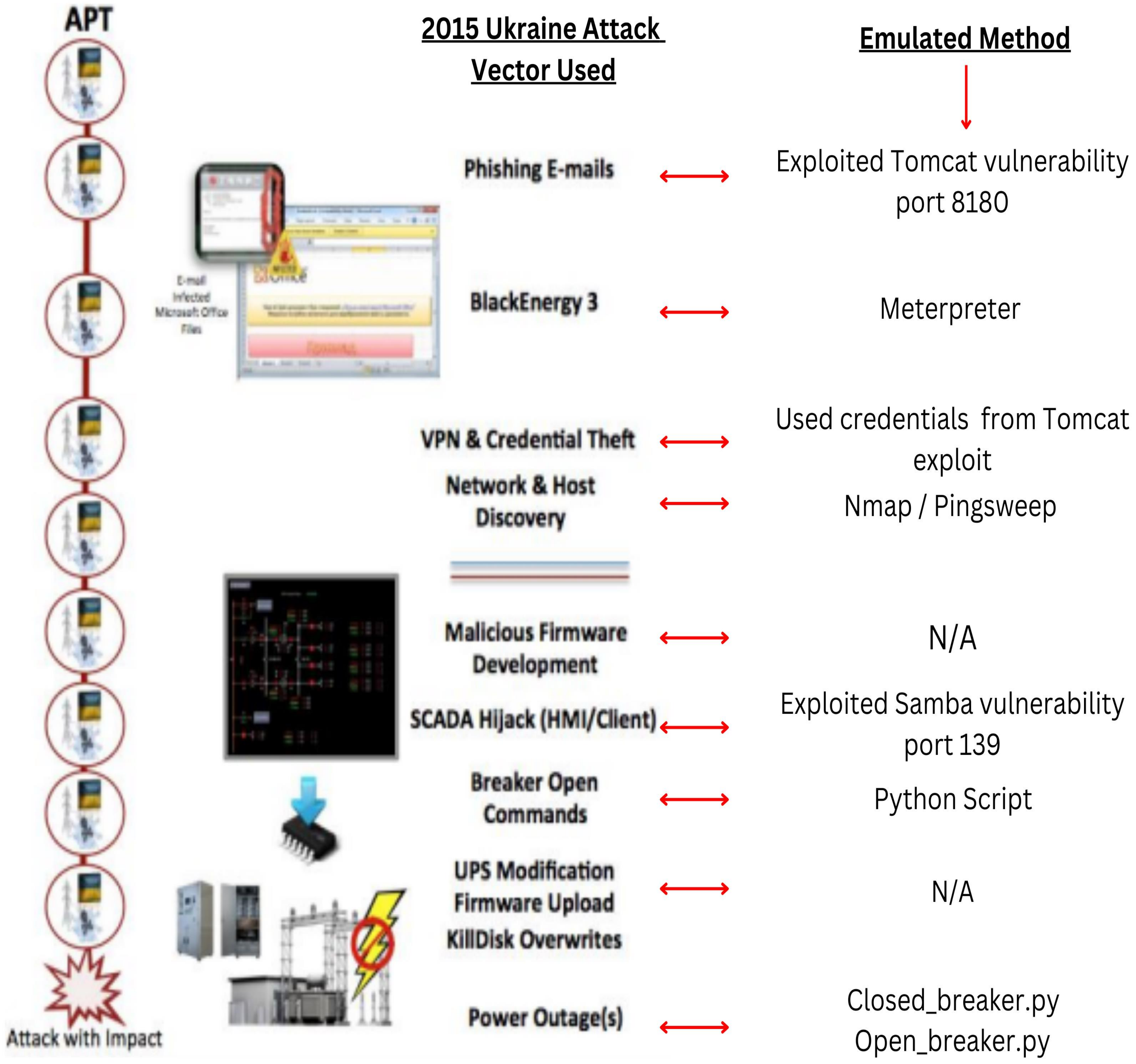

D: Detect the cyber- events with distributed ledger technology
A: Distributed ledger technology rack, B: inside (relays)/ outside (power meters) substation devices rack, C: electrical substation- grid rack
E: Supervise the real-time simulation tests with hardware in the loop
DISTRIBUTED LEDGER TECHNOLOGY (CONTROL CENTER)
A
INSIDE / OUTSIDE SUBSTATION POWER METERS AND RELAYS
B
ELECTRICAL GRID AND SUBSTATION (REAL TIME SIMULATOR)
C
2 1:40:45
2 1:40:45
D
E
I
H
G
F
I: Collect the cyber-events from distributed ledger technology devices
H: Collect traffic from inside and outside substation devices based on IEC61850 and DNP
G: Collect substation inside/ outside device events (COMTRADE files)
F: Collect currents, voltages, breaker states from tests (MATLAB files)

Figure 2. Physical Testbed

Ukraine Attack Kill Chain Emulation Model

The ICS Kill Chain model in *Figure 3* was used to display the different attack vectors used for this attack against the ones used in the 2015 Ukraine attack [1].



2015 Ukraine Attack Vector Used	Emulated Method
Phishing E-mails	Exploited Tomcat vulnerability port 8180
BlackEnergy 3	Meterpreter
VPN & Credential Theft	Used credentials from Tomcat exploit
Network & Host Discovery	Nmap / Pingsweep
Malicious Firmware Development	N/A
SCADA Hijack (HMI/Client)	Exploited Samba vulnerability port 139
Breaker Open Commands	Python Script
UPS Modification Firmware Upload KillDisk Overwrites	N/A
Power Outage(s)	Closed_breaker.py Open_breaker.py

Figure 3. Recreation of attack vectors used

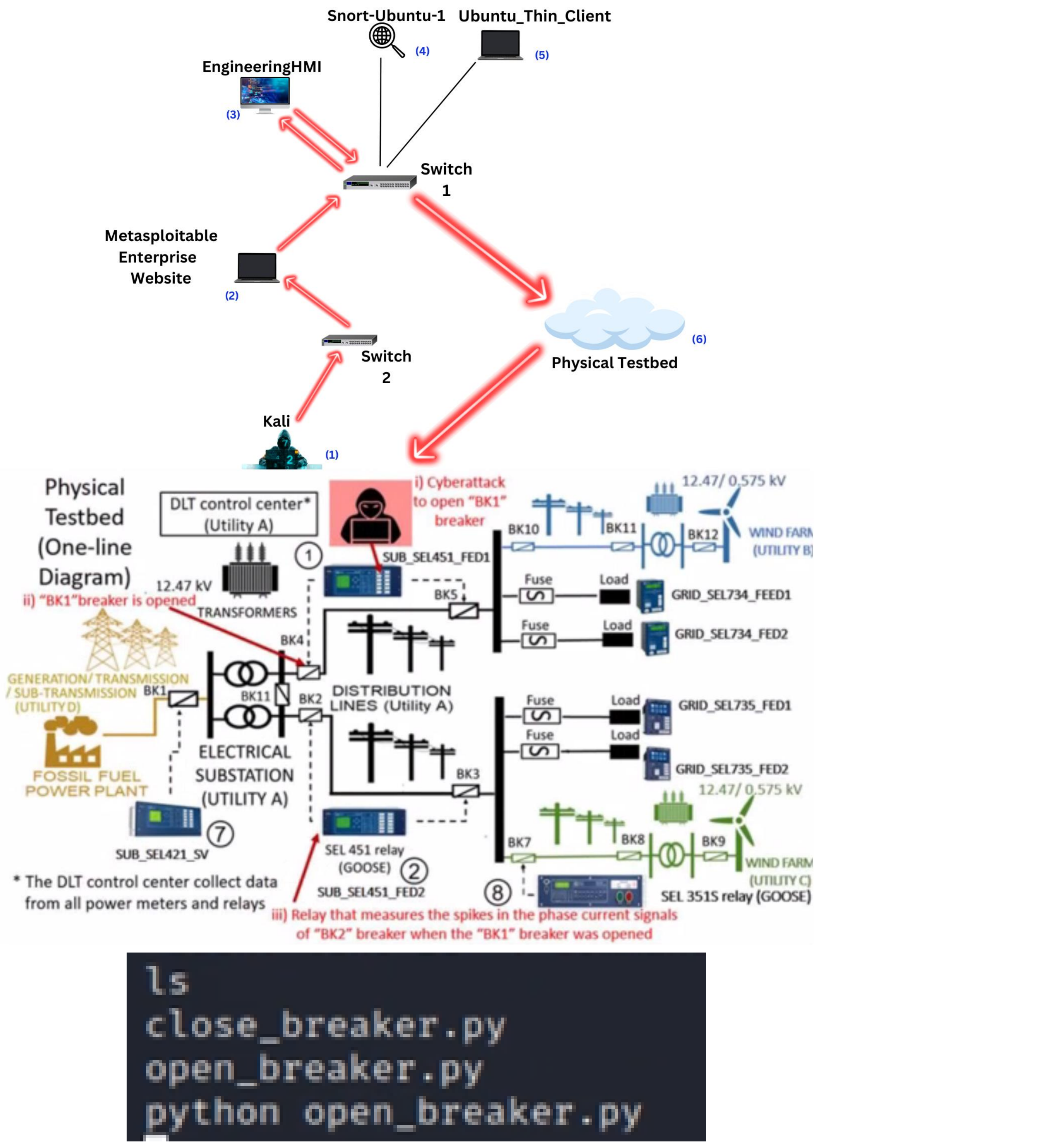
Attacks

STEP 1: Nmap was used from the Kali machine (node1) to scan the IP addresses of the Enterprise Website (node2) and HMI (node3) to obtain open port information and operating system type. The scan revealed a Tomcat Web Vulnerability on port 8180 on the Enterprise Website (node2) and a Samba vulnerability on port 139 for the Human Machine Interface (node3).

STEP 2: Metasploit was used to exploit the Tomcat Web Vulnerability on port 8180 towards the Enterprise Website (node2) resulting in a successful reverse shell.

STEP 3: With the reverse shell, the autoroute command was used to create a pivot to the Human Machine Interface (HMI) to exploit the Samba vulnerability on port 139 based on the Nmap scan in step 1.

STEP 4: A meterpreter session was used to exploit the Samba vulnerability on port 189 which allowed admin privileged access to the Human Machine Interface resulting in the breaker to open as seen in *Figure 4*.


Snort-Ubuntu-1
(4)
Ubuntu_Thin_Client
(5)
EngineeringHMI
(3)
Switch 1
Metasploitable Enterprise Website
(2)
Switch 2
Physical Testbed
(6)
Kali
(1)
Physical Testbed (One-line Diagram)
DLT control center* (Utility A)
i) Cyberattack to open "BK1" breaker
12.47/ 0.575 kV
BK10
BK11
BK12
WIND FARM (UTILITY B)
1
SUB_SEL451_FED1
12.47 kV
ii) "BK1"breaker is opened
TRANSFORMERS
BK5
Fuse
Load
GRID_SEL734_FEED1
GRID_SEL734_FED2
BK4
GENERATION/ TRANSMISSION / SUB-TRANSMISSION (UTILITY D)
BK1
BK11
BK2
DISTRIBUTION LINES (Utility A)
GRID_SEL735_FED1
GRID_SEL735_FED2
FOSSIL FUEL POWER PLANT
ELECTRICAL SUBSTATION (UTILITY A)
BK3
12.47/ 0.575 kV
7
SUB_SEL421_SV
SEL 451 relay (GOOSE)
2
SUB_SEL451_FED2
BK7
BK8
BK9
WIND FARM (UTILITY C)
8
SEL 351S relay (GOOSE)
* The DLT control center collect data from all power meters and relays
iii) Relay that measures the spikes in the phase current signals of "BK2" breaker when the "BK1" breaker was opened

```
ls
close_breaker.py
open_breaker.py
python open_breaker.py
```

Figure 4. Attack process to open breaker

Results and Conclusions

The attack used to gain access to the Human Machine Interface was effective because of the ability to open the breaker. The ICS Kill Chain emulation methods used against the 2015 Ukraine attack were successfully implemented. The Ukraine power grid attack served as a significant reminder of the criticality of safeguarding the United States power grid against potential cyber security threats directed at essential infrastructure in the Americas. Analyzing the tactics employed during those attacks becomes paramount, as it can lead to improved and fortified power grid security measures. By studying these incidents, valuable insights can be gained to better protect and mitigate potential future cyber threats aimed at our vital infrastructure.

References

[1] Lee, R. M., Assante, M. J., & Conway, T. (2016, March 18). Analysis of the Cyber Attack on the Ukrainian Power Grid. Retrieved July 26, 2023, from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Acknowledgements

"This research was supported in part by the U.S. Department of Energy (DOE), Omni Technology Alliance Internship Program. The program is championed by the DOE's Office of Chief Information Officer (OCIO) and represents a partnership with the leadership of the Office of Economic Impact and Diversity, the Office of Science, the Office of Nuclear Energy, and the National Nuclear Security Agency. The program is administered by the Oak Ridge Institute for Science and Education."