Mehran University Research Journal of Engineering and Technology
Vol. 41, No. 1, 202 - 219, January 2022
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: https://doi.org/10.22581/muet1982.2201.20

Intrusion Detection and Prevention against Cyber Attacks for an Energy Management System

Saqib Ali[1], Tahir Nadeem Malik[2]

RECEIVED ON 28.01.2020, ACCEPTED ON 16.12.2020

ABSTRACT

Industrial Microgrids (IμG) are the large-scale buildings fortified with onsite Distributed Generations (DGs), energy storage, and demand response strategies. For optimal handling of these energy resources, storages, and loads to better match the power demand with the generation, a management system is developed termed as Industrial Energy Management System (IEMS). The optimal operation of IEMS depends on the accuracy of information flowing through the communication links between user and IEMS as well as the IEMS and utility grid. Communication links have some associated cybersecurity issues such as unauthorized access, data modification, and disrupt disclosure to change the operating conditions in today's era of computation. The main goal of this paper is to devise a technique to efficiently detect and prevent internal as well as external apparition attempts. For this purpose, an Intrusion Detection and Prevention System (ID/PS) against cyber-attacks is developed using a Linux operating system based on Smooth-sec software. The proposed ID/PS would continuously monitor and record the traffic within the local IμG network to distinguish a legal command from a real attack by decoding the attack packets to create its templates with defined ID/PS rules to take prevention measures and triggered an alert, alarm or Splunk for the security administrator. The devised novel approach significantly contributes to intrusion attention to vulnerabilities and security analysis of cyber secured equipped IEMS for an IμG.

Keywords: Cyber Security, Energy Management System, Industrial Microgrids, Intrusion Detection and Prevention System, Smooth-sec Software

1. INTRODUCTION

In a typical industry, controls, devices, systems, and networks are used to operate. Automate distributed industrial procedures such as measuring, monitoring, internal auditing, non-conformance (corrective and preventive) and records *etc.* are followed. Industrial controls include programmable logic controllers, distributed controls, supervisory controls, energy management control *etc.*

The computerized control provides healthy and safe operating conditions for distributed energy resources, storages, and loads to optimize energy consumption and/or usage and responds to demand response signals termed as energy management control. The Industrial Energy Management System (IEMS) monitors and controls the energy supply to critical processes.

For this reason, the detection and prevention of a security vulnerability may cause this system to become potentially attacked by internal as well as external intruders. Seizing the control and illegal monitoring of the system may cause the entire microgrid (μG) to become paralyzed. This may result not only in economic damage but also the administrator in the control center may not receive important information.

[1] Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan.
Email: saqib.ali@nfciet.edu.pk (Corresponding Author).
[2] Department of Electrical Engineering, HITEC University, Taxila, Pakistan.
Email: tahir.nadeem@hitecuni.edu.pk

The cyberattacks against electrical power grids, industrial control systems and other critical infrastructure have increased in frequency and severity. Businessmen and industrial shareholders/stakeholders are very conscious to take precautionary measures to address internal as well as external cyberattacks related problems before a major catastrophe occurs [1, 2].

For example, in April 2019, the Wall Street Journal published an article about vulnerability in the United States power grid. An unknown external intruder attempted an attack on F-35 databases and destroyed some of the parts of the database [3].

In May 2017, WannaCry ransomware virus software was among one of the largest attacks that were infested in multiple billing companies in India. Distribution Companies in West Bengal State that served approximately 800,000 consumers were attacked. The bill-payment operation had to be suspended due to the external intruder attack for whole day until the back-up data could be restored [4].

In June 2017, a Russian hackers team called Sandworm used an updated ransomware program known as Black-Energy malware package as a cyberattack to hijack the operation and control of power stations in multiple regions of Ukraine's national power company, shutting down the electricity of approximately 225,000 Ukrainians for many hours, but service was restored after 3-6 hours. That was the world's first hacker-caused power outage [5].

In the first half of 2017, a Russia-based hacking group, called Dragonfly 2.0 by security researchers, targeted dozens of Western energy companies, breaking into more than 20 firms' networks and possibly obtaining operational access to some in the US and Turkey [6].

In January 2014, a CIA official said the agency was aware of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities [7].

The above mentioned well known cyber attacks accentuate the fact that the energy control system in a μG or the smart power distribution system is extremely vulnerable to internal as well as external intruders. The μG may be one of the primary targets in the smart energy distribution system for cyber attackers to destroy its electrical power flow. So, it is very difficult to evaluate in profundity to expose existing vulnerabilities in μG components, controls, devices, systems, networks and protocols *etc*. to take precautionary measures against these vulnerabilities and prevent them from being exploited against intruders.

In an old Industrial Control System (ICS), Private Networks (PNWs) are used to communicate the information between different components in the industry. These PNWs are not linked with external networks and are considered as more secure communication links. The cybersecurity of these PNWs can be neglected. However, in this advanced era of communications, a secure internet or intranet is required to monitor the distributed energy generation, storage, and loads in an Industrial Microgrid (IμG).

The hybrid, integrated, and wireless network protocols, schemes, routings, and mechanisms have made the communication system more vulnerable to various cyber-attacks. Therefore, a strategy needs to be devised to manage and secure the customer's sensitive information from un-authorized intruders for the cyber secure communication of data.

In this context, the concept of an Intrusion Detection and Prevention System (ID/PS) against cyber-attacks has been quite beneficial. Intrusion detection and prevention recording of network traffic for Cyphers is essential for a possible intruder attack. During monitoring, it distinguishes the licensed user or malicious attacker to detect and prevent possible internal and/or external intrusions in the communication channels. When the network detects potentially treacherous activity, it not only takes action to stop the intruder before it can perform serious damage but also takes some action to adopt precautionary measures against it by dropping malicious packets, blocking network traffic or resetting the connections *etc*. The devised technique also sends an alert to the administrators about potentially malicious activity.

A modern industrial infrastructure requires a regular and continuous monitoring based communication network without any type of interruption between the user and IEMS as well as the IEMS and the utility grid to provide reliable continuous two-way power supply and to prevent attacks. For this purpose, the proposed technique is devised for a cyber secured IEMS using Linux operating system based Smooth-sec software that contains a complete package of network security tools [8, 9] as shown in Fig. 1:.

The complete architectural view of cyber secured IEMS for an IμG is shown in Fig. 2:. Energy management system controls the customer's stakes such as energy cost and emission minimization, and comfort level maximization by taking tariff and irradiance data, and customer preferences as input from customers, utility and weather servers through a Secure Communication Link (SCL) between user and IEMS as well as IEMS and utility grid. User-IEMS link may be developed by using either Bluetooth or Zigbee. Any intrusion to this channel to change the information may be termed as an internal intrusion, however, unauthorized access to the IEMS-utility link is termed as an external intrusion. The optimal operation of IEMS depends on the accuracy of information flowing to and from the cyber secure IEMS control module. However, external, or/and internal intruders may change the accuracy resulting in in-optimal scheduling of μG components. To overcome this threat, a cybersecurity mechanism is developed to detect and prevent unlicensed internal as well as external access to the industrial local area network. The literature survey related to the cybersecurity of an industrial control system is described in detail as:

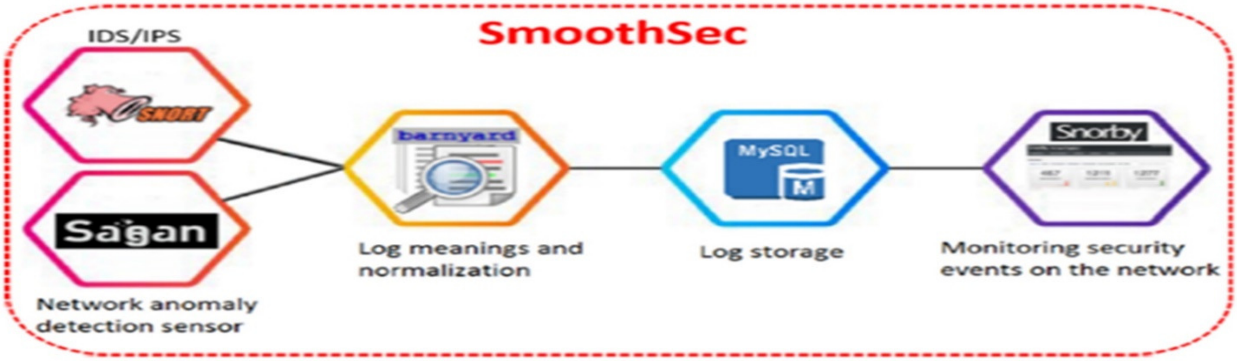

SmoothSec
IDS/IPS
SNORT
Sagan
Network anomaly detection sensor
barnyard
Log meanings and normalization
MySQL
M
Log storage
Snorby
Monitoring security events on the network

Fig. 1: Complete layout of Smooth-sec software

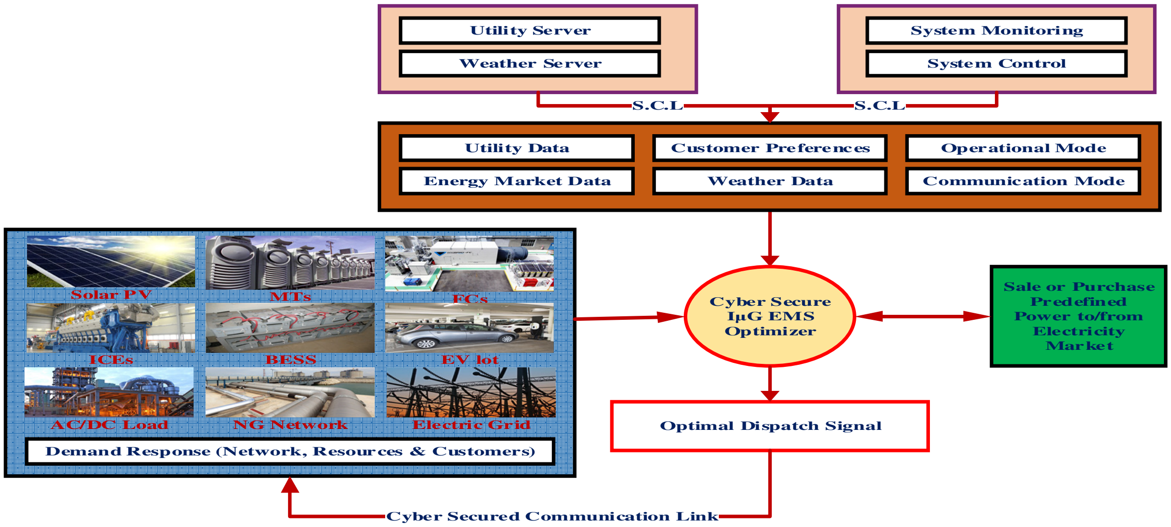


Fig. 2: Pictorial view of cyber secured EMS for IμG

Anuebunwa *et al.* [10] analyzed the impact of cyber-attack on load scheduling applications in a residential building. Attacker interfered with critical data including dynamic pricing information and load profile *etc*. The objective function included the impact on occupant comfort, cost, and load variations. The proposed framework was based on the Genetic Algorithm (GA). The devised scheme detected the false data injection to warn the system administrator to take remedial measures.

Ylmaz *et al.* [11] developed a cyber secure mechanism for an ICS to protect it from the most devastating threat such as a Denial of Service (DoS) attack. Programmable logic controller (S-7 1200), an industrial component was attacked. The attack was analyzed in three phases. The first phase was termed as "attack stage". In this phase, the nature of the attack and its effect was assessed. In the second phase, that is "reconnaissance stage", analyzed captured packets, and in the third phase called "detection stage", patterns related to the attack w\were created. The results showed the effects of the attack, attack packets source IP address, the acquired signature, and the rule information to detect and prevent a PLC from the intruders [11].

The authors in [8] proposed a rule-based testbed in Smooth-sec software to detect the active attacks on programmable logic controllers in an ICS by using the mirroring technique. Under this strategy, the system compared the attack log file with the signature file residing in the snort library to discriminate between the normal and obnoxious data to generate a warning message for the system administrator.

Hwang [12] highlighted various security challenges and threats *i.e.* physical attacks, cyber-attacks, or natural disasters which could lead to infrastructural failure, blackouts, energy theft, customer privacy breach and endangered safety of operating personnel, *etc*. The authors also proposed a framework that could identify the security level, source, and cause of threat and the impact of the attack. The devised technique identified and cleared the threat [12].

The researchers in [13] developed an Intrusion Detection System (IDS) for continuously monitoring network traffic and efficiently detecting any intruder from inside or outside attack to enhance the security of an information system. The subject to the attacker was a single computer or the entire network. Intrusion detection system functionality, classification, techniques, and efficiency were described in detail. The simulation was performed under VMware software and consisted of three main devices: 1) an intruder device used as a web vulnerability scanner, 2) an online attacked server that is XAMMP software, and 3) the IDS performing as smooth-sec functioning under Linux Debian, Suricata IDS engine and Snorby. The attack was launched on the server IP address, the IDS generated the real-time alerts and displayed the same on the user console clearly.

Kravchik and Shabtai [14] proposed an efficient anomaly detection and scoring method for ICS by using the 1-D convolutional neural networks and under complete autoencoders based on neural networks. The testbed was developed for secure water treatment at the Singapore University of Technology and Design. The dataset used named "The BATADAL dataset" represented a water distribution network controlled by nine PLCs. Based on experiments, the results showed that three public datasets were utilized to maintain simplicity, short training, small footprint, and generality. The results also demonstrated that by using frequency domain analysis, anomalies and attack detection could easily be explored to pinpoint the specific attack location.

Zhang *et al.* [15] developed a multilayer, data-driven cyber-attack defense mechanism to enhance the cybersecurity for an ICS by applying the defense-in-depth concept. To detect and prevent the attacks traditional, supervised, and unsupervised models were used. The proposed IDS suggested that yje bagging had low false and missed alarms for attacks. Furthermore, an auto-associative Kernel regression model was used to detect physically impactful cyber-attacks before significant consequences occur by utilizing the network, system, and process data. That was claimed as a promising solution for safeguarding an ICS [15].

Literature survey shows that for an IEMS, an ID/PS ID/PS against cyber-attacks has not been devised to attain the objectives of securing the communication channel of an IμG. The rest of the paper is organized as: Section 2 explains intrusion detection and prevention mechanism, Section 3 presents experimental environment, analyses, and results and Section 4 concludes the paper.

2. PROPOSED INTRUSION DETECTION AND PREVENTION MECHANISM

The proposed technique has three steps: attack, detection, and prevention as shown in Fig. 3. In the first step, an intruder launches an attack at the input ports of the IEMS module. In the second step, the ID/PS residing in IEMS continuously monitors data ports to differentiate between normal and abnormal packets. For this purpose, in the third step, the template of the data packet is created. This template contains the IP address and decoded version of the information.

Apart from research work available in the literature on IEMS, the cybersecurity issues are particularly important to secure its control module from malicious attacks in an IμG. Such cyber-attacks may modify or alter the information of a load profile and load shapes that are highly confidential and competition sensitive as they may indicate the types, times, and durations of equipment and loads.

The cyber-attack on the data communication channel between the IEMS and the utility may alter the data as well as its confidentiality. As the wireless or wired links remain under the threat of continuous unauthorized intrusion from external and/or internal intruders that may alter the parameters, for instance, weather and utility data resulting in the non-optimal schedule of μG components. The non-optimal schedule of the industrial process leads to major economic losses. To address such an undesirable scenario, a strategy for a cybersecurity breach, needs to be devised in an IμG.

Under the view of the above-mentioned literature, this paper proposes a cyber secure equipped IEMS in smooth-sec software to detect and prevent unlicensed internal and external intrusion to secure the communication link between the customers and IEMS module as well as IEMS and the utility grid. Such a cyber-secure communication link masks the IEMS module to avoid malfunction due to internal and/or external intrusions.

The hourly energy demand of each sub-process in a cement factory situated in Taxila, Pakistan, is taken as an example as shown in Fig. 4. The manufacturing facility functions daily in two shifts of 12 h each. The load pattern reveal that most of the processes such as finishing work are carried out during the daytime. The security of this load profile is vital for the innocuous operation of the IEMS's components. It is, therefore, essential to implement cyber-secured IEMS that protect the private data of the industry, avert un-authorized access and provide authentication, authorization, and audit-ability to the communication infrastructure in an IμG resulting in erroneous energy consumption cost.

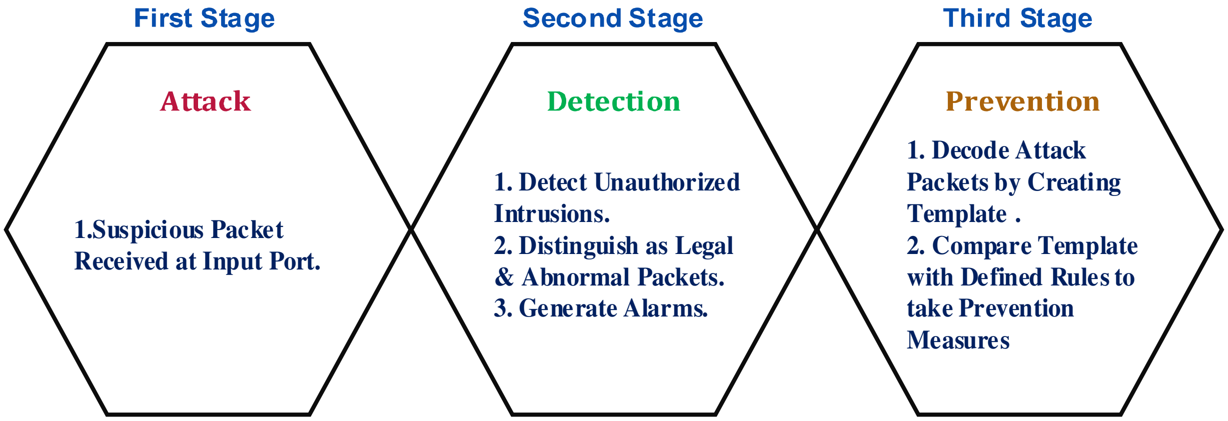

First Stage
Second Stage
Third Stage
Attack
1.Suspicious Packet Received at Input Port.
Detection
1. Detect Unauthorized Intrusions.
2. Distinguish as Legal & Abnormal Packets.
3. Generate Alarms.
Prevention
1. Decode Attack Packets by Creating Template .
2. Compare Template with Defined Rules to take Prevention Measures

Fig. 3: Stages for proposed detection and prevention system

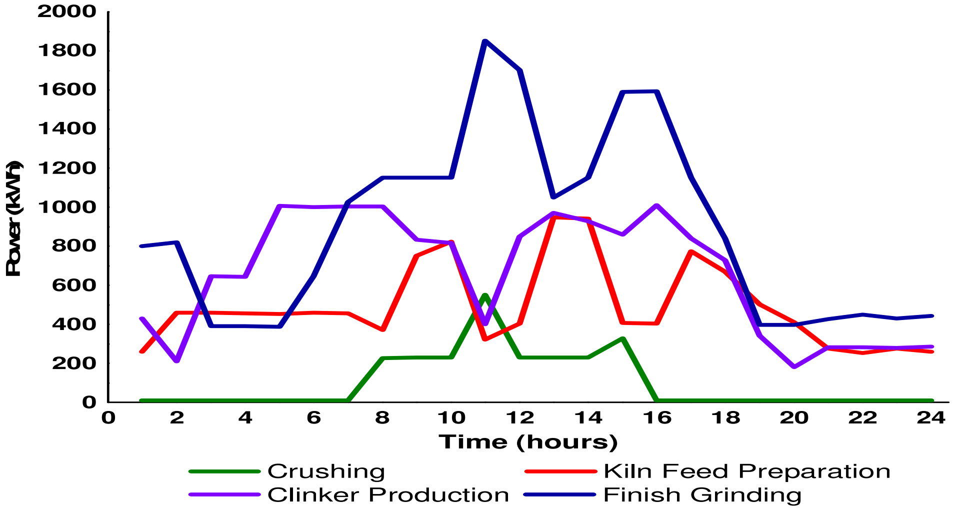


Fig. 4: Normal 24-h Average load profile

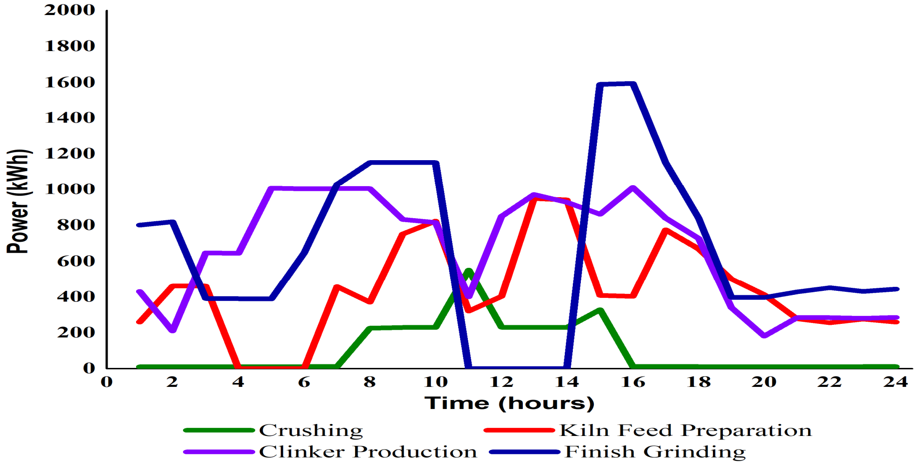


Fig. 5: After attack 24-h load profile

The DoS attack is carried out on the real-time load profile data and due to this cyber-attack, it modifies this load profile as can be seen in Fig. 5. The attack is carried out on the processes' load of the considered cement factory that is kiln feed preparation and finishing grinding. The attacker or intruder is successful in altering the load profile data and disturbs the whole manufacturing process that may cause a huge disturbance in the monitoring, operation as well as control of the communication and may even fails the entire IEMS module. To secure the IEMS from these types of attacks, a strategy is developed in this paper for this class of customers.

Literature review [16-20] shows that there are various types of attack named as (a) Denial-of-Service (DoS), (b) Man-in-the-Middle (MitM), (c) drive-by attack, (d) password attack, (e) Structured Query Language (SQL) injection attack and (f) zero-day exploit *etc*.

In the DoS attack [21, 22], individual or multiple attackers (s) transmit a flood of information to a target server/ router either from within customer premises or from outside. Under such conditions, the system either crashes or denies service to the authorized user resulting in inconvenience to the customers and malfunction of the IEMS module.

In a man-in-the-middle attack [23, 24], an unlicensed intruder intermeddles or eavesdrops on the communicating parties to alter the information, thereby, modifying the actual meaning of the message.

Such an attractor may reside inside or outside of the μG. Under such conditions, EMS may receive erroneous energy prices from the utility server (external intruder), weather data from the meteorology department (external intruder), and customer preferences (internal intruder).

In a drive-by attack [25], an external or internal intruder may access and install malicious malware in the IEMS module. Under such situations, the intruder controls the EMS to improperly schedule the μG components and reach in-optimal decisions.

Under password attacks [26, 27], internal or external intruders decrypt the password to gain access to the EMS to alter its operational behavior to reach an in-optimal solution.

In the SQL injection attack [28], intruders access the database to act as a system administrator and may either change or wipe out the entire data.

In zero-day exploit [29], cybercriminals scan the weaknesses or vulnerability of the EMS software and develop tools to exploit them.

Among the above-mentioned attacks, DoS and change of passwords have been the most commonly occurring [30]. Therefore, this paper proposes a cybersecurity technique to detect and prevent these attacks for the secure operation of IEMS.

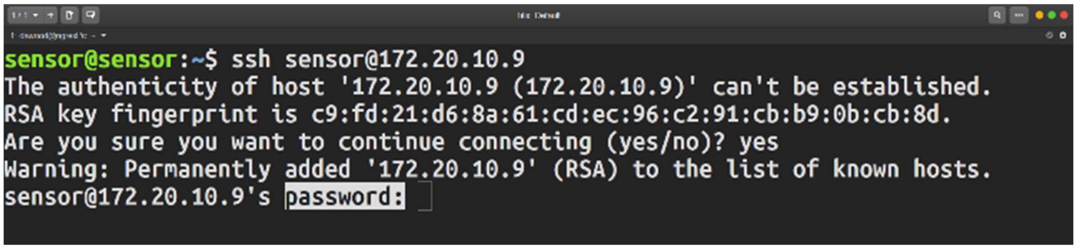
Literature shows that internal intrusion proves more threatening compared to external attacks, however, the scope of devised technique must deal with both internal as well as external intrusions within the local area network of an IμG.

3 EXPERIMENTAL ENVIRONMENT, ANALYSIS, AND RESULTS

The rest of this subsection discusses the two cases, the first one without the devised technique and the second one describes the implementation perspective of the proposed ID/PS technique.

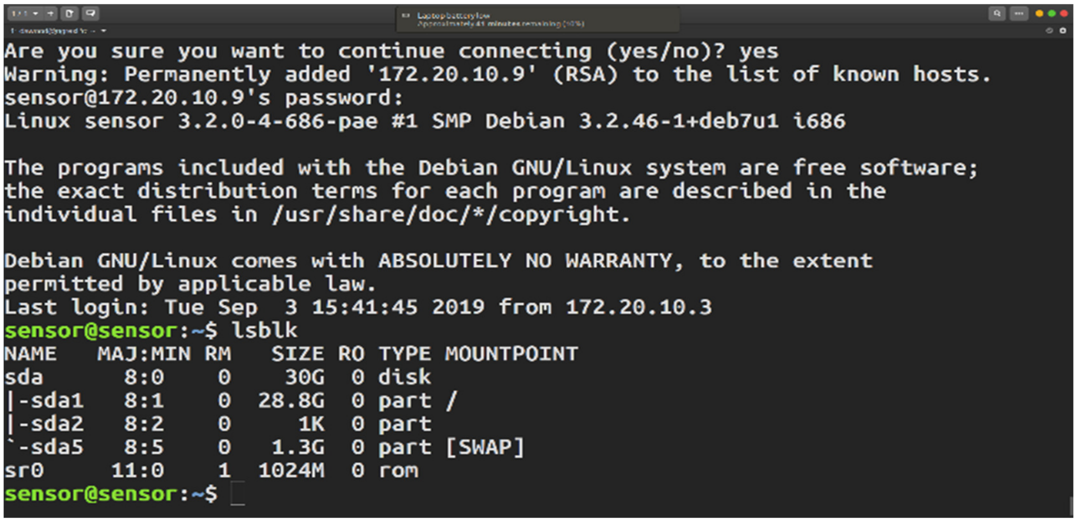
A. CASE-1: *Without Proposed Intrusion Detection and Prevention Technique*

In this case, (without the proposed scheme), the DoS attack is carried out from a single external source on the IEMS control with IP address 172.20.10.9. The external source lies outside the IμG premises intending to access the IEMS memory module for the DoS attack. Denial of service may be in the form of change in energy tariff, weather data, customer preferences, on/off signals of building components such as the battery, EV lot, and DGs, and even maybe in the form of process shutdown. Under such conditions, the IEMS sub-optimally dispatches consequently resulting in loss to the building owner. The external attacker launches a DoS attack on the IEMS module to establish a connection using the “ssh protocol” shown in Fig. 6. In response to this, the local area network of the IμG denies establishing such a link between attacker and host (IEMS). However, after this failure, the attacker generates a random list of its fingerprints and applies it to target IEMS. In case the features of any fingerprint match with the features of the IEMS memory module, that fingerprint will be permanently added to the list of known hosts. After this, the attacker does not require any permission in the form of a password for entry in the IEMS. As the attacker enters into the IEMS it gains access to the information of the memory shown in Fig. 7, to alter stored data and functional status of the individual IμG components to undesirably turn them on or off as shown in Fig. 8. The intruder may even turn off the IEMS module itself by applying the “Sudo shutdown” command. Under such a situation, IEMS will no more be available for optimal dispatch of IμG components.



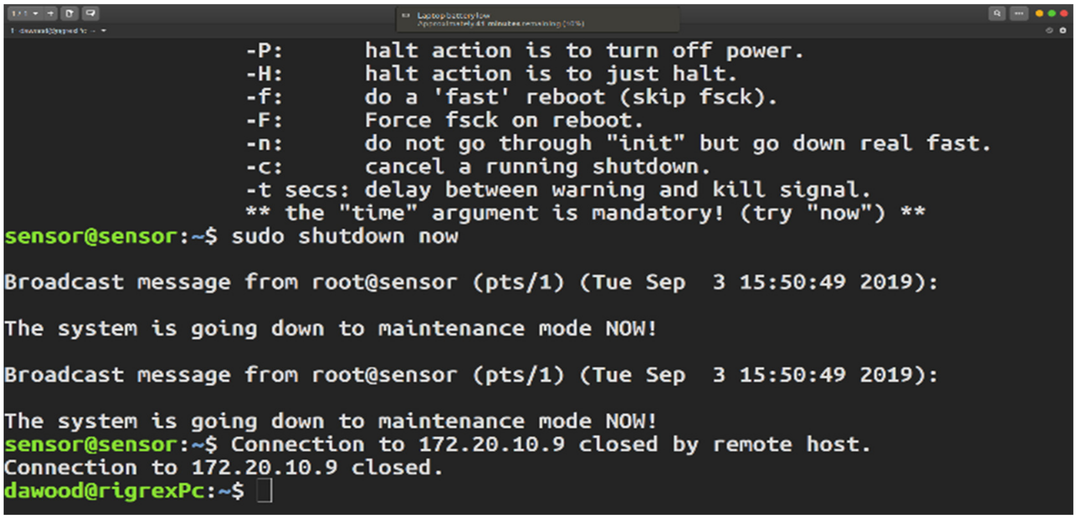
```
sensor@sensor:~$ ssh sensor@172.20.10.9
The authenticity of host '172.20.10.9 (172.20.10.9)' can't be established.
RSA key fingerprint is c9:fd:21:d6:8a:61:cd:ec:96:c2:91:cb:b9:0b:cb:8d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.9' (RSA) to the list of known hosts.
sensor@172.20.10.9's password:
```

Fig. 6: DoS attack carried out from a single source on the IEMS control



```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.9' (RSA) to the list of known hosts.
sensor@172.20.10.9's password:
Linux sensor 3.2.0-4-686-pae #1 SMP Debian 3.2.46-1+deb7u1 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep  3 15:41:45 2019 from 172.20.10.3
sensor@sensor:~$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0    30G  0 disk
|-sda1   8:1    0  28.8G  0 part /
|-sda2   8:2    0     1K  0 part
`-sda5   8:5    0   1.3G  0 part [SWAP]
sr0     11:0    1  1024M  0 rom
sensor@sensor:~$
```

Fig. 7: IEMS control due to a DoS attack leads to significant problems



```
                  -P:      halt action is to turn off power.
                  -H:      halt action is to just halt.
                  -f:      do a 'fast' reboot (skip fsck).
                  -F:      Force fsck on reboot.
                  -n:      do not go through "init" but go down real fast.
                  -c:      cancel a running shutdown.
                  -t secs: delay between warning and kill signal.
                  ** the "time" argument is mandatory! (try "now") **
sensor@sensor:~$ sudo shutdown now

Broadcast message from root@sensor (pts/1) (Tue Sep  3 15:50:49 2019):

The system is going down to maintenance mode NOW!

Broadcast message from root@sensor (pts/1) (Tue Sep  3 15:50:49 2019):

The system is going down to maintenance mode NOW!
sensor@sensor:~$ Connection to 172.20.10.9 closed by remote host.
Connection to 172.20.10.9 closed.
dawood@rigrexPc:~$
```

Fig. 8: IEMS control shutting down due to DoS attack

The rest of the subsection describes the intrusion detection and prevention strategy to avoid such a scenario.

B. CASE-2: *With Proposed Intrusion Detection and Prevention Technique*

For the validation of the proposed ID/PS scheme, the system shown in Fig. 9. is designed in smooth-sec software [8]. One IEMS control computer with IP address 172.20.10.9 is used (installed in Smooth-sec software as a sensor to protect it from intruders) from which remote commands and control of the IEMS are generated. One personal computer in which smooth-sec is installed as a console as can be found in the literature that Smooth-sec software functions in two modes: 1) as a sensor representing the cybersecurity part of the IEMS module and 2) as the console. The industrial energy management system acts as a target of an attacker or intruder, whereas the console functions as an antivirus capable of detecting and eradicating the attack. Both sensor and console having different IP addresses reside in two separate computers as shown in Figs. 10 -11.

Fig. 12 displays the “Snorby web dashboard” of the normal traffic before the attacks. Snorby (part of smooth-sec) is a modern front-end web interface application that is free, open-source, and highly competitive, specially designed for monitoring network security. Practically it lies under the jurisdiction of the system administrator for network traffic monitoring purposes. Window in Fig. 12. shows that currently there is no attack of the low, medium, and high severity level on the IEMS module.

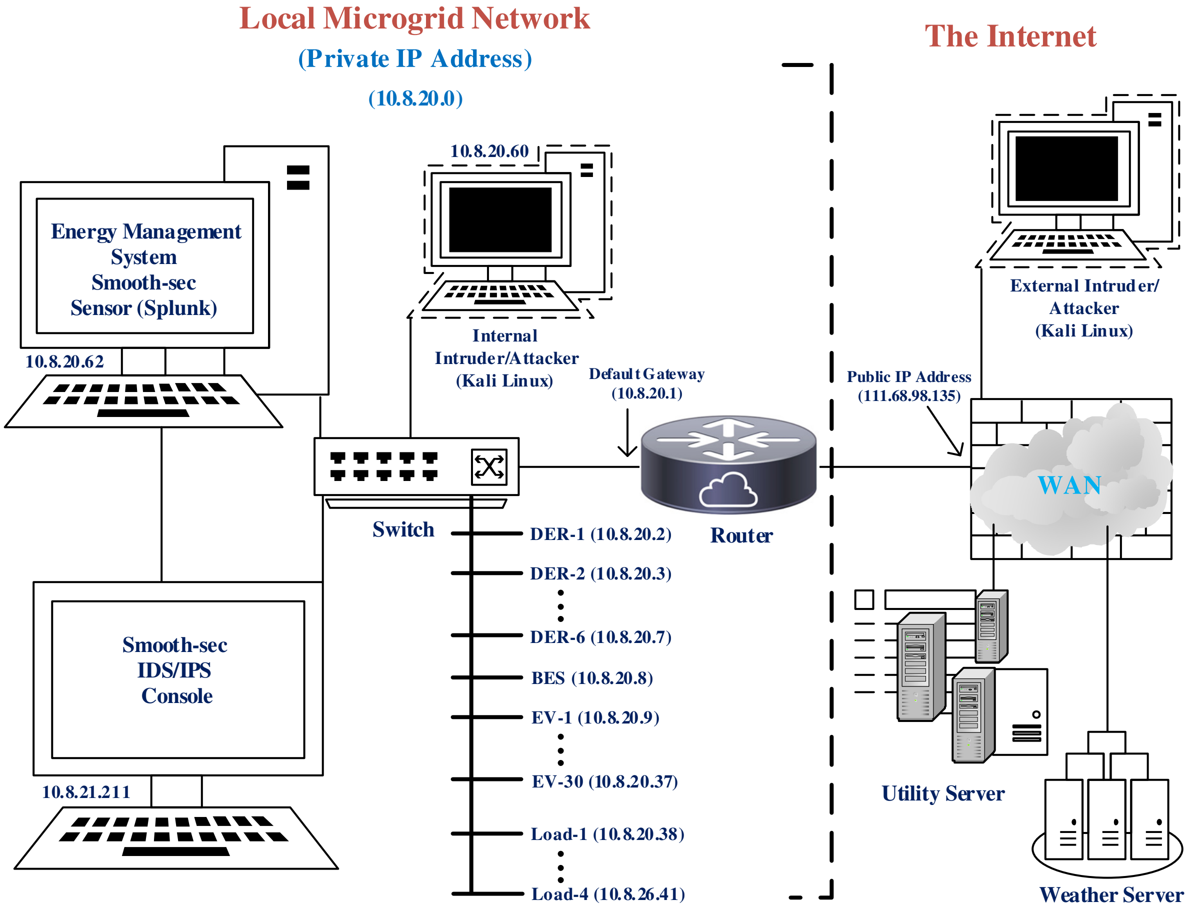
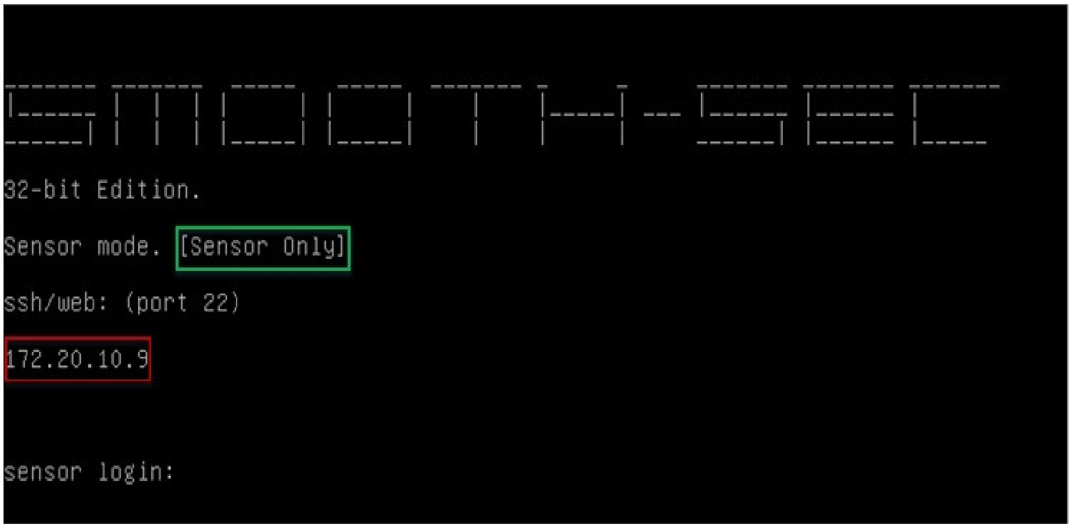
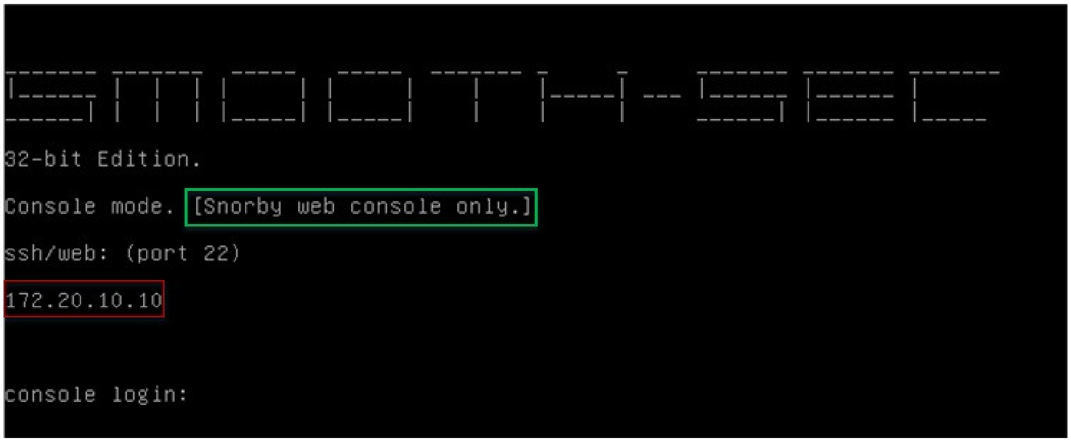


Fig. 9: Proposed industrial microgrid network topology



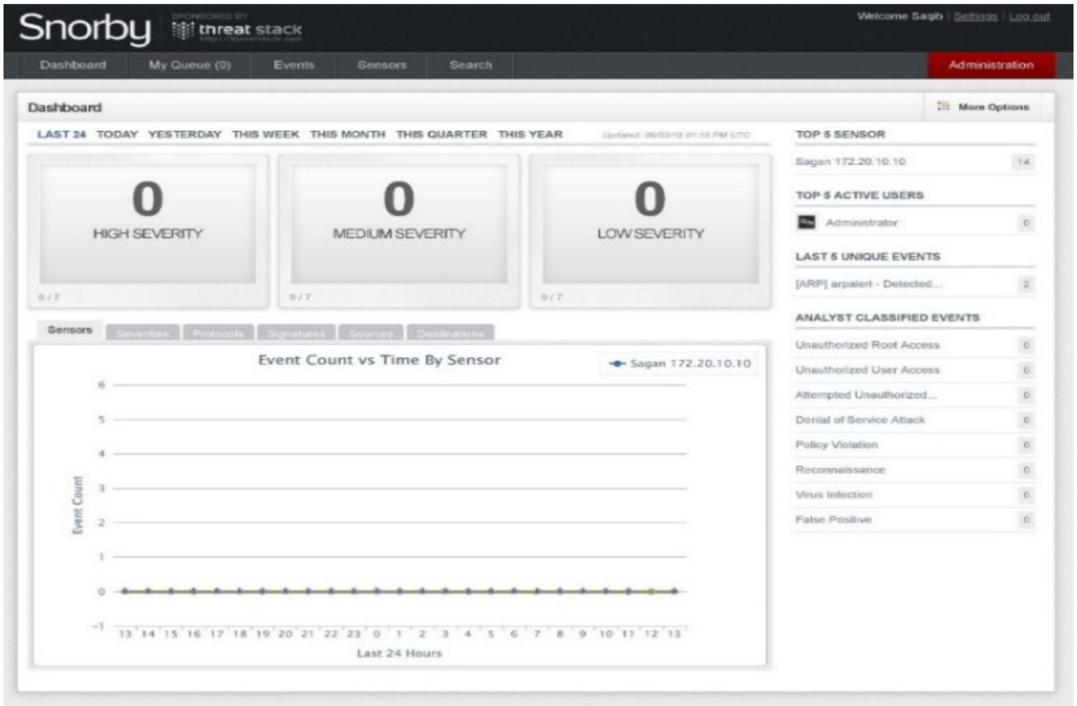
```
------ ------- ----- ----- ------ -   -  ------ ------ ------
|----- |  |  | |   | |   |   |    |---|  --  |----- |----- |
-----| |  |  | |___| |___|   |    |   |      -----| |_____ |_____
32-bit Edition.

Sensor mode. [Sensor Only]

ssh/web: (port 22)

172.20.10.9


sensor login:
```

Fig. 10: Smooth-sec installed as sensor



```
32-bit Edition.

Console mode. [Snorby web console only.]

ssh/web: (port 22)

172.20.10.10


console login:
```

Fig. 11: Smooth-sec installed as console



TOP 5 SENSOR
Sagan 172.20.10.10 14

TOP 5 ACTIVE USERS
Administrator 0

LAST 5 UNIQUE EVENTS
[ARP] arpalert - Detected... 2

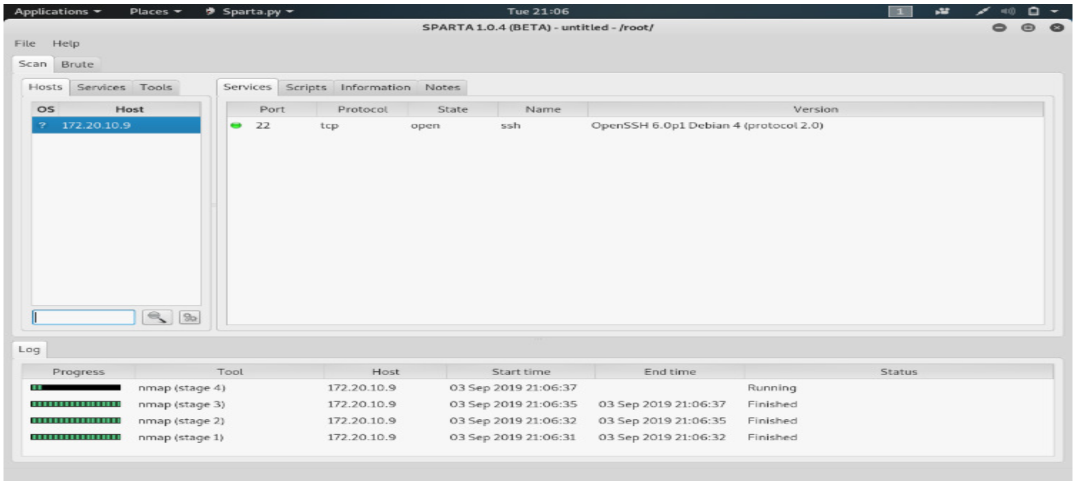
ANALYST CLASSIFIED EVENTS
Unauthorized Root Access 0
Unauthorized User Access 0
Attempted Unauthorized... 0
Denial of Service Attack 0
Policy Violation 0
Reconnaissance 0
Virus Infection 0
False Positive 0

Fig 12: Snorby web dashboard to show normal traffic before the attack

The two black-screened computers are shown in Fig. 9 with IP address 192.168.43.224 acting as an internal intruder/attacker and the IP address of the external intruder may or may not be known. Linux based operating system termed Kali Linux 4.18.10 is installed to generate malware data packets as shown in Fig. 13. The window shown in Fig. 14, displays the stages and types of attacks by using Sparta 1.0.4(BETA) named as “open with telnet (DoS attack)”, “open with ssh client as root (password mismatch attack)”, open with Netcat, send to Brute, run Nmap five stages (scripts) on a port, and grab banner. Sparta, a GUI-based application used to test the network infrastructure by injecting the penetration tester by setting up commands and tools from the toolkit to focus on the analyzed results. As can be seen that the IEMS control acts as a host with IP address is 172.20.10.9, port number 22, TCP protocol and the version open SSH 6.0p1 Debian 4(protocol 2.0) are being attacked by the Kali Linux based operating system.

Differentiation between normal and abnormal data is carried out by comparing the IP address of the arrived packet with the IP addresses of the authorized persons. These authorized IP addresses reside in the console library. Whenever, IP address does not match with any of the authorized IP addresses, an alarm triggers, and a prevention system subsequently blocks the attacker's port as shown in Fig. 15. However, if the attacker copies the IP address of authorized persons residing in the console library, through IP spoofing [31] and impersonates to be the privileged individual; the impersonated IP address matches. In such a case, the attacker gains access to the IEMS of the IμG and tries to enter the control module through a password. In response to this, the Smooth sec installed as a sensor in the IEMS informs the system administrator that an unauthorized person is trying to enter into the IEMS by impersonating as an authorized person. Under such a situation, the attacker will be blocked by the sensor as shown in Fig. 16.

Along with this, another brute-force attack is also applied that is termed as "send to Brute", it is a password cracking attack that snips the hidden pages and content from the Web applications. The attack is basically "a hit and try" approach and analyzes the response until you succeed. When this attack is applied to the IEMS control, the proposed technique will not only stop it but also inverse host lookup failed for the unknown internal as well as external intruders as shown in Fig. 17.

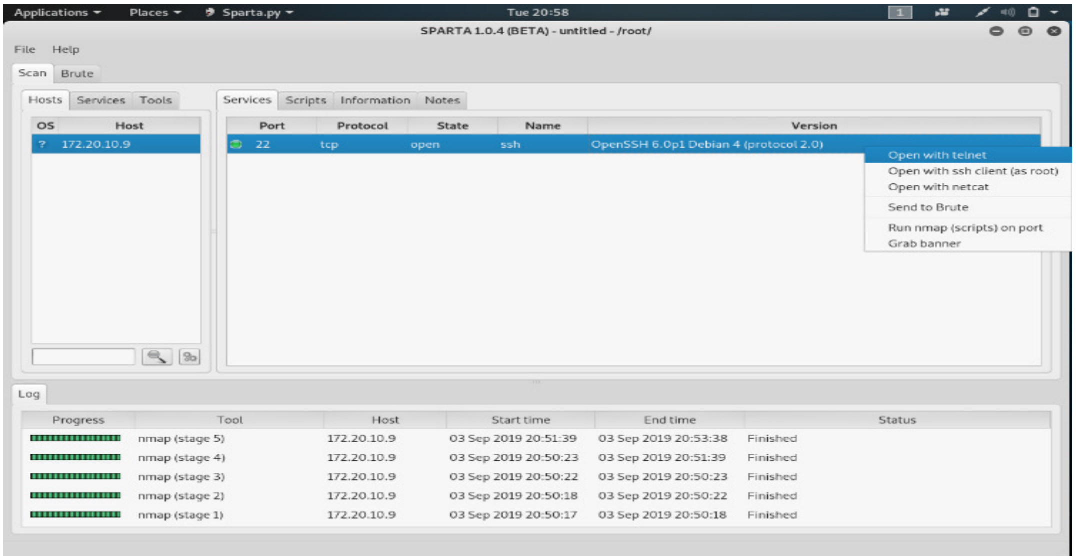


OS	Host
?	172.20.10.9

Port	Protocol	State	Name	Version
22	tcp	open	ssh	OpenSSH 6.0p1 Debian 4 (protocol 2.0)

Progress	Tool	Host	Start time	End time	Status
	nmap (stage 4)	172.20.10.9	03 Sep 2019 21:06:37		Running
	nmap (stage 3)	172.20.10.9	03 Sep 2019 21:06:35	03 Sep 2019 21:06:37	Finished
	nmap (stage 2)	172.20.10.9	03 Sep 2019 21:06:32	03 Sep 2019 21:06:35	Finished
	nmap (stage 1)	172.20.10.9	03 Sep 2019 21:06:31	03 Sep 2019 21:06:32	Finished

Fig. 13: Kali Linux operating system installed for attacks at IEMS

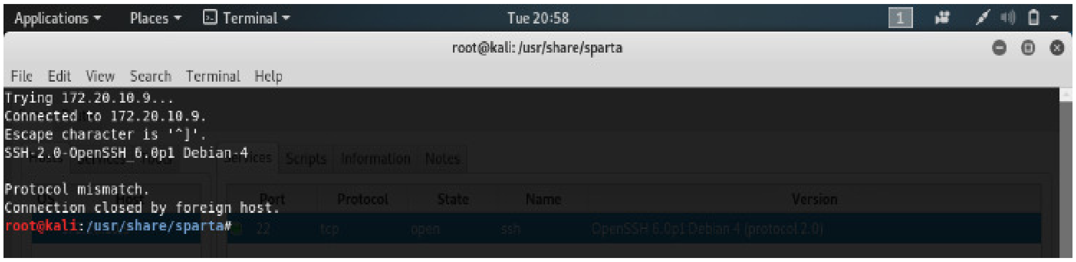


OS	Host
?	172.20.10.9

Port	Protocol	State	Name	Version
22	tcp	open	ssh	OpenSSH 6.0p1 Debian 4 (protocol 2.0)

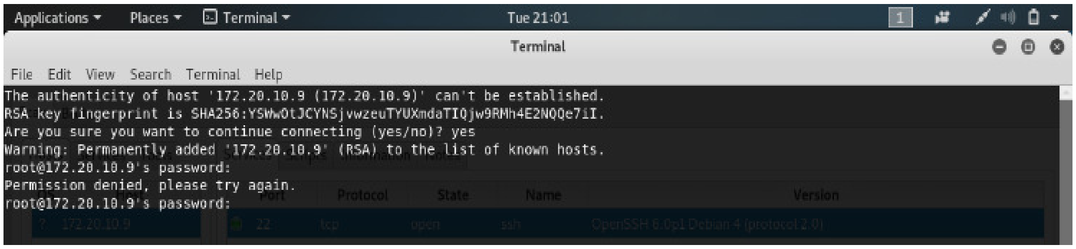
Progress	Tool	Host	Start time	End time	Status
	nmap (stage 5)	172.20.10.9	03 Sep 2019 20:51:39	03 Sep 2019 20:53:38	Finished
	nmap (stage 4)	172.20.10.9	03 Sep 2019 20:50:23	03 Sep 2019 20:51:39	Finished
	nmap (stage 3)	172.20.10.9	03 Sep 2019 20:50:22	03 Sep 2019 20:50:23	Finished
	nmap (stage 2)	172.20.10.9	03 Sep 2019 20:50:18	03 Sep 2019 20:50:22	Finished
	nmap (stage 1)	172.20.10.9	03 Sep 2019 20:50:17	03 Sep 2019 20:50:18	Finished

Fig. 14: Stages and types of attacks implemented through Kali Linux


Applications
Places
Terminal
Tue 20:58
root@kali: /usr/share/sparta
File Edit View Search Terminal Help

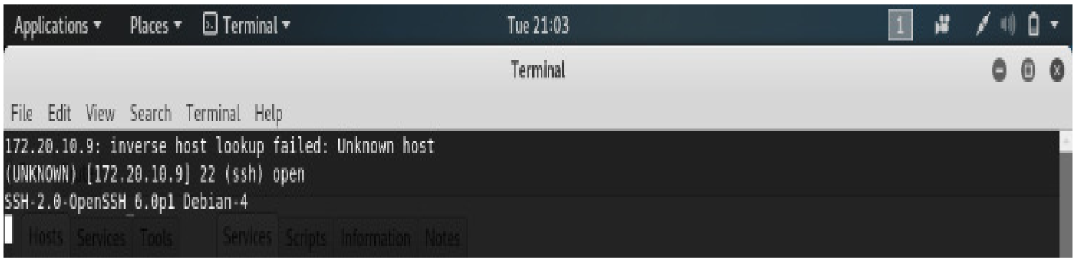
```
Trying 172.20.10.9...
Connected to 172.20.10.9.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.0p1 Debian-4

Protocol mismatch.
Connection closed by foreign host.
root@kali:/usr/share/sparta#
```

Fig. 15: Open with telnet attack (protocol mismatch)



```
The authenticity of host '172.20.10.9 (172.20.10.9)' can't be established.
RSA key fingerprint is SHA256:YSWwOtJCYNSjvwzeuTYUXmdaTIQjw9RMh4E2NQQe7iI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.9' (RSA) to the list of known hosts.
root@172.20.10.9's password:
Permission denied, please try again.
root@172.20.10.9's password:
```

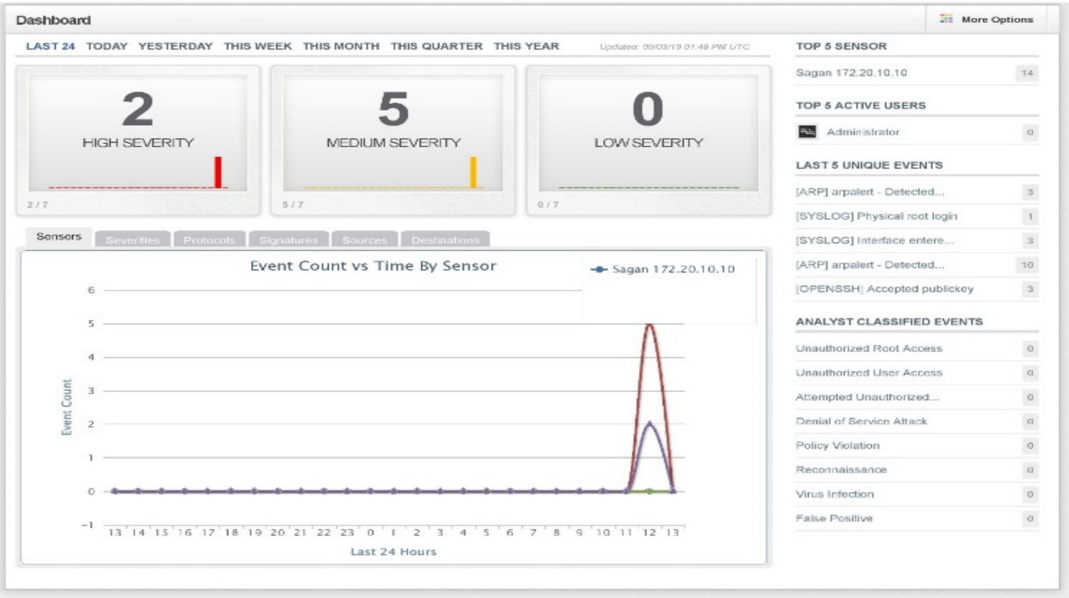
Fig. 16: Open with ssh client (as root) attack (permission denied)



```
172.20.10.9: inverse host lookup failed: Unknown host
(UNKNOWN) [172.20.10.9] 22 (ssh) open
SSH-2.0-OpenSSH_6.0p1 Debian-4
```

Fig. 17: Send to Brute (unknown host)

Fig. 18 shows abnormal activities and generates a Splunk and/or alert/alarm by using the alarm generation mechanism after the attacks are being applied through the Kali Linux operating system.



2 HIGH SEVERITY 2 / 7

5 MEDIUM SEVERITY 5 / 7

0 LOW SEVERITY 0 / 7

TOP 5 SENSOR	
Sagan 172.20.10.10	14

TOP 5 ACTIVE USERS	
Administrator	0

LAST 5 UNIQUE EVENTS	
[ARP] arpalert - Detected...	3
[SYSLOG] Physical root login	1
[SYSLOG] Interface entere...	3
[ARP] arpalert - Detected...	10
[OPENSSH] Accepted publickey	3

ANALYST CLASSIFIED EVENTS	
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0
False Positive	0

Fig. 18: Snorby web dashboard shows abnormal traffic after the attack

Fig. 19 shows the alarm generation mechanism that simply reads and records the log files of all the packets arriving on the IEMS control and compares it with the rules that reside in the snort library patterns. If the packets match with any of the snort's ruleset, it will block this packet and an alarm/alert or Splunk is generated for the administrator. That is two high-level severities, and five medium level severities are blocked through the console sensor named sagan with IP 172.20.10.10. It will also draw a graph of the last 24-hours vs event count (attacks). The graph depicts that from 11:00 to 13:00 hours the events took placed.

The following Figs. 20-24 show attack severity level (as high, medium, and low), protocols (as TCP, UDP, and ICMA), signatures (as SYSLOG: interface entered promiscuous mode, ARP: detecting IP change, and OpenSSH: secured a communication channel over an unsecured network), source information of Internal attack (with IP: 10.147.20.186) and external attack (with IP: 192.168.43.224 and 192.168.43.194), and the destinations (IEMS control with IP: 172.20.10.9).

In the analysis environment, Snort and Sagan are the intruder detection sensors as shown in Fig. 25. A snort sensor is a packet sniffer that continuously follows or monitores the network traffic coming and going from different outsider networks in real-time, scrutinizing abnormal movements closely to detect hazardous payload or suspicious anomalies and generates alerts and/or alarms for the administrator at Snorby web application. In this context, it detects the signature through the attack rules definitions in it and matches the same signature of Snort. The maximum 14 event counts took place on the IEMS control with IP address 172.20.10.9 from Snort sensor through the eth0 interface that is 33.30%. Whereas the Sagan sensor perceives network incongruities and changes in accordance with the well-defined rules by monitoring the components of network traffic. It protects from internal as well as external intruders by using the Sagan intruder detection system. It also distinguishes between normal and abnormal data packets and identifies the threatening source that makes it easier for the security administrator to react rapidly to anomalous network packets or activities. The alerts based on sagan are generated when the disturbance is created in the configuration of the local area network, adding a new device, and operators check that these suspicious activities are illegal or legitimate and can hurriedly execute a blocking or permission action.

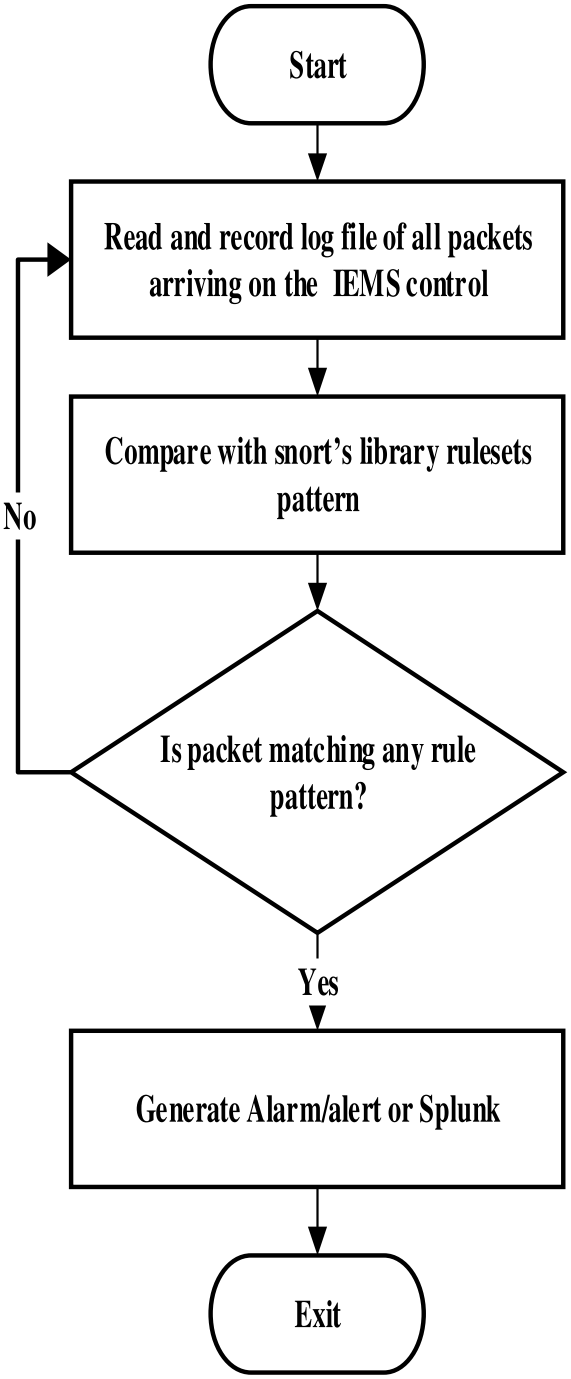

Start
Read and record log file of all packets arriving on the IEMS control
Compare with snort's library rulesets pattern
No
Is packet matching any rule pattern?
Yes
Generate Alarm/alert or Splunk
Exit

Fig. 19: Alarm generation mechanism to the administrator

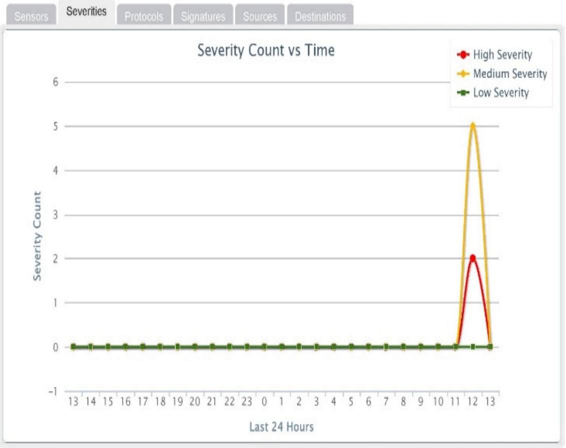


Fig. 20: Attacks severities level

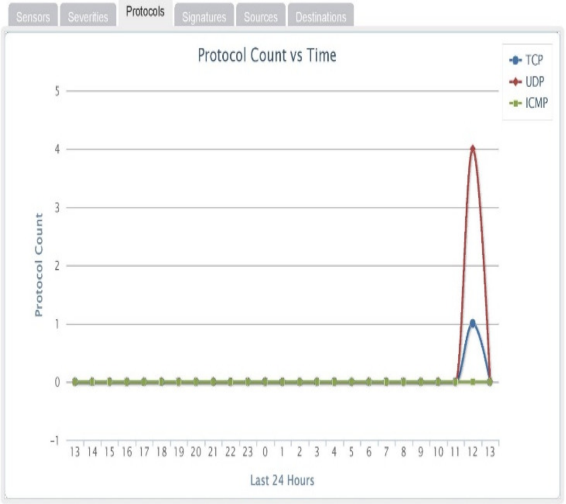


Fig. 21: Attack protocols

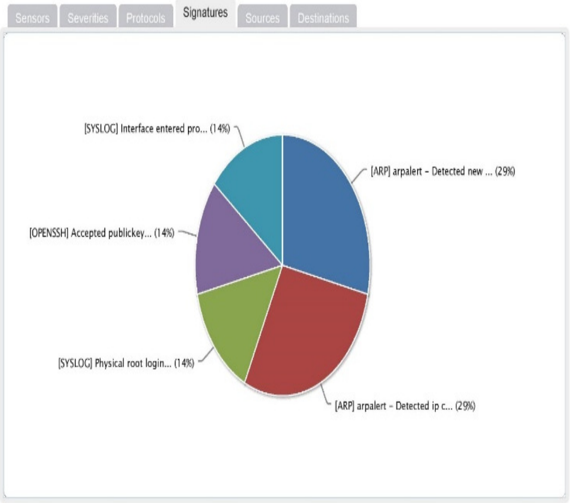


Fig. 22: Attack signatures

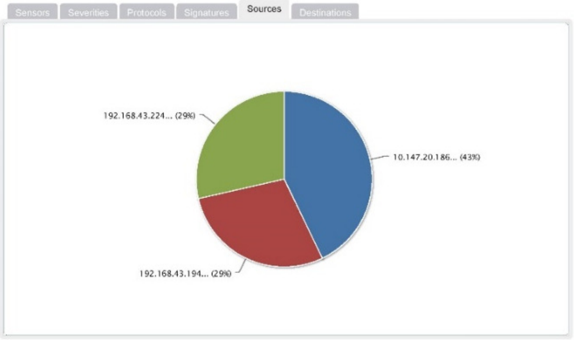


Fig. 23:Internal and external attack source information

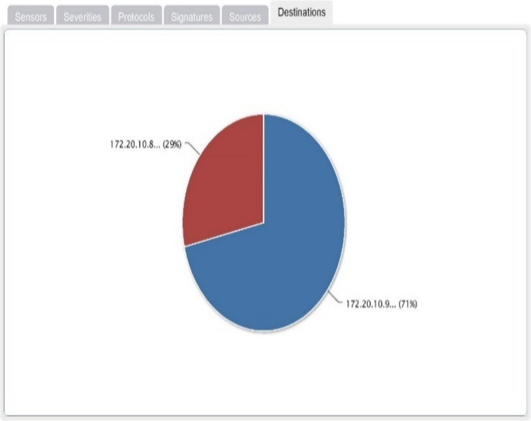
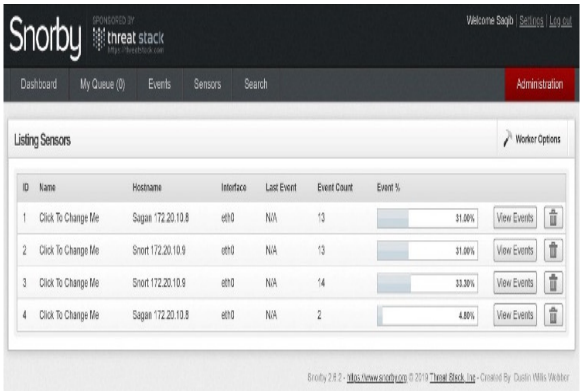


Fig. 24: Attack destinations (IEMS control)



Listing Sensors

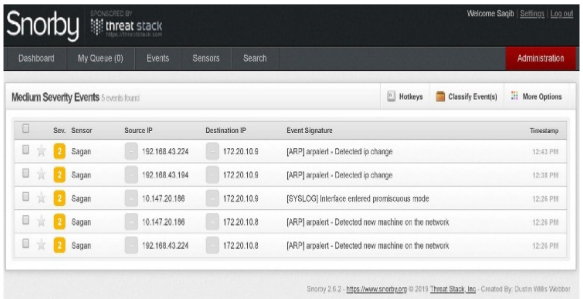
ID	Name	Hostname	Interface	Last Event	Event Count	Event %		
1	Click To Change Me	Sagan 172.20.10.8	eth0	N/A	13	31.00%	View Events	
2	Click To Change Me	Snort 172.20.10.9	eth0	N/A	13	31.00%	View Events	
3	Click To Change Me	Snort 172.20.10.9	eth0	N/A	14	33.30%	View Events	
4	Click To Change Me	Sagan 172.20.10.8	eth0	N/A	2	4.80%	View Events	

Snorby 2.6.2 - https://www.snorby.org © 2019 Threat Stack, Inc - Created By Dustin Willis Webber

Fig. 25: Sensor used to detect the attackers

The medium severities events increased as the attack packets coming from the internal and/or external intruders matched with the Sagan library rule set signatures. When these packets were explored on the Snorby web page, it was found that it had the external intruder source IP: 192.168.43.224 and 192.164.43.194, internal intruder source IP:10.147.20.186 and destination host (IEMS control)

IP: 172.20.10.9, and the information about the suspicious event signatures. The events detected by the Sagan sensor included the change in IP address, interfaced entered in promiscuous mode, and detected new machine on the internet *etc* as shown in Fig. 26.

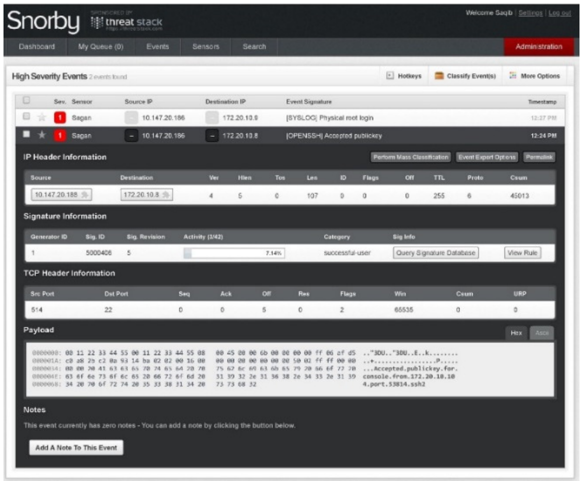

Snorby
SPONSORED BY threat stack https://threatstack.com
Welcome Saqib | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Medium Severity Events 5 events found
Hotkeys
Classify Event(s)
More Options

	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□ ☆	2	Sagan	192.168.43.224	172.20.10.9	[ARP] arpalert - Detected ip change	12:43 PM
□ ☆	2	Sagan	192.168.43.194	172.20.10.9	[ARP] arpalert - Detected ip change	12:38 PM
□ ☆	2	Sagan	10.147.20.186	172.20.10.9	[SYSLOG] Interface entered promiscuous mode	12:26 PM
□ ☆	2	Sagan	10.147.20.186	172.20.10.8	[ARP] arpalert - Detected new machine on the network	12:26 PM
□ ☆	2	Sagan	192.168.43.224	172.20.10.8	[ARP] arpalert - Detected new machine on the network	12:26 PM

Snorby 2.6.2 - https://www.snorby.org © 2019 Threat Stack, Inc - Created By: Dustin Willis Webber

Fig. 26: Attack event packets

Fig. 27 shows the high severities events packet carried out from the Kali Linux operating system as an intruder with the IP address 10.147.20.186 to IEMS control with IP address 172.20.10.9 by using 102nd as a communication port. These pieces of information of the intruder can be seen on the Snorby web interface that provides great convenience to the network security administrator. It can also be informed to the administrator that whether the commands and control signal were varied out by an authorized user or by a nasty attacker. Fig. 27 has four major pieces of information *i.e*. IP header information, signature information and the TCP header information, and the payload of the attacked packet. The payload is the actual data of the attacked packet that causes major harm to the destination host (IEMS control).


Snorby
SPONSORED BY threat stack https://threatstack.com
Welcome Saqib | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
High Severity Events 2 events found
Hotkeys
Classify Event(s)
More Options
Perform Mass Classification
Event Export Options
Permalink
Hex
Ascii

	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□ ☆	1	Sagan	10.147.20.186	172.20.10.9	[SYSLOG] Physical root login	12:27 PM
■ ★	1	Sagan	10.147.20.186	172.20.10.8	[OPENSSH] Accepted publickey	12:24 PM

IP Header Information

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
10.147.20.188	172.20.10.8	4	5	0	107	0	0	0	255	6	45013

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (3/42)	Category	Sig Info	
1	5000406	5	7.14%	successful-user	Query Signature Database	View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
514	22	0	0	5	0	2	65535	0	0

Payload

```
0000000: 00 11 22 33 44 55 00 11 22 33 44 55 08  00 45 00 00 6b 00 00 00 00 ff 06 af d5  .."3DU.."3DU..E..k........
000001A: c0 a8 2b c2 0a 93 14 ba 02 02 00 16 00  00 00 00 00 00 00 00 50 02 ff ff 00 00  ..+................P.....
0000034: 00 00 20 41 63 63 65 70 74 65 64 20 70  75 62 6c 69 63 6b 65 79 20 66 6f 72 20  ...Accepted.publickey.for.
000004E: 63 6f 6e 73 6f 6c 65 20 66 72 6f 6d 20  31 39 32 2e 31 36 38 2e 34 33 2e 31 39  console.from.172.20.10.10
0000068: 34 20 70 6f 72 74 20 35 33 38 31 34 20  73 73 68 32                             4.port.53814.ssh2
```

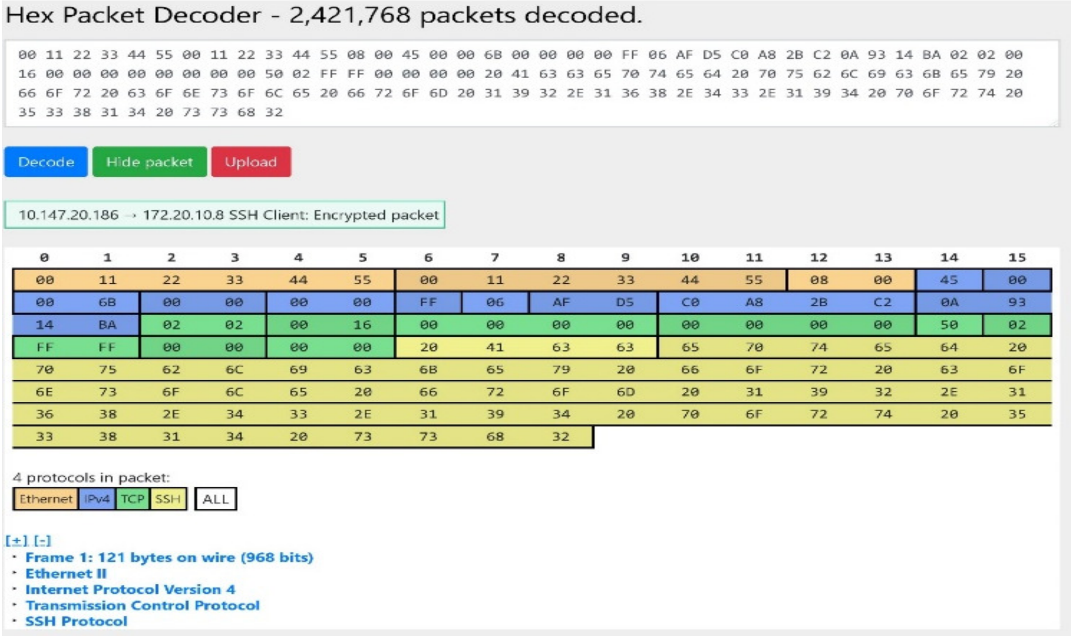
Notes

This event currently has zero notes - You can add a note by clicking the button below.

Add A Note To This Event

Fig. 27: Attack event analysis packet

The payload was separated and analyzed by transferring a copy by using the Hex packet decoder to explore its features. The attacked packet is extracted from the IμG local area network that flows towards the IEMS control. The content and its features obtained by examining the apprehended attack packet via Wireshark can be seen in Fig. 28 and Table 1.


Hex Packet Decoder - 2,421,768 packets decoded.

```
00 11 22 33 44 55 00 11 22 33 44 55 08 00 45 00 00 6B 00 00 00 00 FF 06 AF D5 C0 A8 2B C2 0A 93 14 BA 02 02 00
16 00 00 00 00 00 00 00 00 50 02 FF FF 00 00 00 00 20 41 63 63 65 70 74 65 64 20 70 75 62 6C 69 63 6B 65 79 20
66 6F 72 20 63 6F 6E 73 6F 6C 65 20 66 72 6F 6D 20 31 39 32 2E 31 36 38 2E 34 33 2E 31 39 34 20 70 6F 72 74 20
35 33 38 31 34 20 73 73 68 32
```

10.147.20.186 → 172.20.10.8 SSH Client: Encrypted packet

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	11	22	33	44	55	00	11	22	33	44	55	08	00	45	00
00	6B	00	00	00	00	FF	06	AF	D5	C0	A8	2B	C2	0A	93
14	BA	02	02	00	16	00	00	00	00	00	00	00	00	50	02
FF	FF	00	00	00	00	20	41	63	63	65	70	74	65	64	20
70	75	62	6C	69	63	6B	65	79	20	66	6F	72	20	63	6F
6E	73	6F	6C	65	20	66	72	6F	6D	20	31	39	32	2E	31
36	38	2E	34	33	2E	31	39	34	20	70	6F	72	74	20	35
33	38	31	34	20	73	73	68	32							

4 protocols in packet:

[+] [-]

- Frame 1: 121 bytes on wire (968 bits)
- Ethernet II
- Internet Protocol Version 4
- Transmission Control Protocol
- SSH Protocol

Fig. 28: Attack packet payload (sample and feature)

Table 1: Attack Packet Payload (Sample and Features)

Payload	
Features	**Content**
Encapsulation type	Ethernet (1)
Frame No., length, Protocols	1, 121 bytes (968 bits), eth:ethertype:ip:tcp:ssh
Captured length	121 bytes (968 bits)
Protocols in frame	eth:ethertype:ip:tcp:ssh
Type	0100 .... = Version: 4, IPv4(0x0800)
Identification	0x0193 (403)
Flags	PSH, ACK
Source, Destination IP address	10.147.20.186, 172.20.10.8
Source, destination port	514,22
Flags	PSH, ACK
Attack signature	65 20 66 72 6f 6d 20 31
Data	74 79 3d 65 74 68 30 2c 20 76 65 6e 64 6f 72 3d 22
Packet Length	(encrypted): 20416363
Encrypted Packet	65707465642070756 26c69636b657920666f7220636f6e73...

4 CONCLUSION

This paper proposes an intrusion detection and prevention system for the cyber secured IEMS in an IμG. The industrial microgrid has a local area network to communicate with its resources, storage, and loads. The security of IEMS has been extremely vital as the invasion of an internal or external intruder negatively affects the optimal performance of the IEMS module. Therefore, this work proposes an ID/PS scheme. The proposed security approach is validated in smooth-sec software and results are described in detail. The simulation shows that DoS and password attacks are successfully detected and prevented. The outcome of this work justifies practical implementation of a cyber secured IEMS in an industrial microgrid.

ACKNOWLEDGMENT

The research has been executed under the worthy guidance of Prof. Dr. Tahir Nadeem Malik for microgrid based green energy project. Proposed control may be manufactured by utility companies for cyber secured consumption management of large-scale manufacturing facilities.

REFERENCES

1. Paine J., "System and Method for Cyber Security Threat Detection". ed: Google Patents, 2020.
2. Stanovich M. J. *et al.*, "Development of a smart-grid cyber-physical systems testbed," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, 2013, pp. 1-6.
3. Stupp C., "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," *The Wall Street Journal,* Vol. 30, 2019.
4. Mohurle S., Patil M., "A brief study of wannacry threat: Ransomware attack 2017," *International Journal of Advanced Research in Computer Science,* Vol. 8, No. 5, 2017.
5. Sullivan J. E., Kamensky D., "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal,* Vol. 30, No. 3, pp. 30-35, 2017.
6. Kshetri N., Voas J., "Hacking power grids: A current problem", *Computer,* Vol. 50, No. 12, pp. 91-95, 2017.
7. Nikitakos N., Mavropoulos P., "Cyberspace as a State's Element of Power," in *Cyber-Development, Cyber-Democracy and Cyber-Defense*: Springer, pp. 259-277, 2014.
8. Yılmaz E. N., Gönen S., "Attack detection/prevention system against cyber attack in industrial control systems", *Computers and Security,* Vol. 77, pp. 94-105, 2018.
9. Muñoz J.B., "Aplicación para la monitorización y defensa de sistemas Linux," 2012.
10. Anuebunwa U. R., Rajamani H.-S., Abd-Alhameed R., Pillai P., "Investigating the Impacts of Cyber-Attacks on Pricing Data of Home Energy Management Systems in Demand Response Programs," in *2018 IEEE Power &*

Energy Society General Meeting (PESGM), 2018, pp. 1-5: IEEE.

11. Ylmaz E. N., Ciylan B., Gönen S., Sindiren E., Karacayılmaz G., "Cybersecurity in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect," in *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, 2018, pp. 81-85: IEEE.
12. Hwang Y. H., "IoT security & privacy: threats and challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*, 2015, pp. 1-1: ACM.
13. A. B. A. N. M. Ahmed Abdelrahman Eltom, "Intrusion Detection Systems," *International Journal of Modern Communication Technologies & Research (IJMCTR),* vol. 2, no. 9, September 2014 2014.
14. Kravchik M., Shabtai A., "Efficient Cyber Attacks Detection in Industrial Control Systems Using Lightweight Neural Networks", *arXiv preprint arXiv:1907.01216,* 2019.
15. Zhang F., Kodituwakku H. A. D. E., Hines W., Coble J.B., "Multi-Layer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System and Process Data", *IEEE Transactions on Industrial Informatics,* 2019.
16. Maglaras L., Ferrag M. A., Derhab A., Mukherjee M., Janicke H., Rallis S., "Threats, Protection, and Attribution of Cyber Attacks on Critical Infrastructures," *arXiv preprint arXiv:1901.03899,* 2019.
17. Awan J. H., Memon S., Memon S., Pathan K. T., Arijo N. H., "Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities", *Mehran University Research Journal of Engineering and Technology,* Vol. 37, No. 2, pp. 359-366, 2018.
18. Javaid Q., Awan M. D., Naqvi S. H. A., "Securing gateways within clustered power centric network of nodes", *Mehran University Research Journal of Engineering and Technology,* Vol. 35, No. 1, pp. 53-62, 2016.
19. Javaid Q., Yasmeen H., Shah M. A., Kamran M., Sohail A., "Dissecting the security and protection issues in pervasive computing", *Mehran University Research Journal of Engineering and Technology,* Vol. 37, No. 2, pp. 241-256, 2018.
20. Takahashi H., Lakhani U., Raza A., "Knowledge Upload Service Using Semantic-Based Categorization," *Mehran University Research Journal of Engineering and Technology,* Vol. 38, No. 4, pp. 999-1008, 2019.
21. Shaji R. S., Dev V. S., Brindha T., "A methodological review on attack and defense strategies in cyber warfare", *Wireless Networks,* Vol. 25, No. 6, pp. 3323-3334, 2019.
22. Velliangiri S, Karthikeyan P., Kumar V. V., "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks", *Journal of Experimental & Theoretical Artificial Intelligence,* pp. 1-20, 2020.
23. Adams K., "Detecting and preventing man-in-the-middle attacks on an encrypted connection," ed: Google Patents, 2019.
24. Hayashi M., Vázquez-Castro Á., "Physical Layer Security Protocol for Poisson Channels for Passive Man-in-the-Middle Attack," *IEEE Transactions on Information Forensics and Security,* Vol. 15, pp. 2295-2305, 2020.
25. Singhal M., "Analysis and Categorization of Drive-By Download Malware Using Sandboxing and Yara Ruleset", 2019.
26. Pinkas B., Sander T., "Secure authentication systems and methods," ed: Google Patents, 2019.
27. Bodkhe U., Chaklasiya J., Shah P., Tanwar S., Vora M., "Markov model for password attack prevention", *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*, 2020, pp. 831-843: Springer.
28. Raut S., Nikhare A., Punde Y., Manerao S., Choudhary S., "A Review on Methods for Prevention of SQL Injection Attack", 2019.
29. Stellios I., Kotzanikolaou P., Psarakis M., "Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things", *Security and Privacy Trends in the Industrial Internet of Things*, pp. 47-68, Springer, 2019.
30. Uma M., Padmavathi G., "A Survey on Various Cyber Attacks and their Classification," *IJ Network Security,* Vol. 15, No. 5, pp. 390-396, 2013.
31. Ramos M. F., Dalmazo B. L., Nobre J. C., "A Proposal for IP Spoofing Mitigation at Origin in

Homenet Using Software-Defined Networking," I*nternational Conference on Computational Science and Its Applications*, 2019, pp. 179-192: Springer.