Scientific Research Publishing

Communications and Network, 2024, 16, 108-134
https://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

# Optimization of Stealthwatch Network Security System for the Detection and Mitigation of Distributed Denial of Service (DDoS) Attack: Application to Smart Grid System

**Emmanuel S. Kolawole, Penrose S. Cofie, John H. Fuller, Cajetan M. Akujuobi, Emmanuel A. Dada, Justin F. Foreman, Pamela H. Obiomon**

Electrical and Computer Engineering Department, Prairie View A&M University, Prairie View, TX, USA
Email: ekolawoles2011@yahoo.com

**How to cite this paper:** Kolawole, E.S., Cofie, P.S., Fuller, J.H., Akujuobi, C.M., Dada, E.A., Foreman, J.F. and Obiomon, P.H. (2024) Optimization of Stealthwatch Network Security System for the Detection and Mitigation of Distributed Denial of Service (DDoS) Attack: Application to Smart Grid System. *Communications and Network*, **16**, 108-134.
https://doi.org/10.4236/cn.2024.163006

**Received:** June 14, 2024
**Accepted:** August 27, 2024
**Published:** August 30, 2024



## Abstract

The Smart Grid is an enhancement of the traditional grid system and employs new technologies and sophisticated communication techniques for electrical power transmission and distribution. The Smart Grid's communication network shares information about status of its several integrated IEDs (Intelligent Electronic Devices). However, the IEDs connected throughout the Smart Grid, open opportunities for attackers to interfere with the communications and utilities resources or take clients' private data. This development has introduced new cyber-security challenges for the Smart Grid and is a very concerning issue because of emerging cyber-threats and security incidents that have occurred recently all over the world. The purpose of this research is to detect and mitigate Distributed Denial of Service [DDoS] with application to the Electrical Smart Grid System by deploying an optimized Stealthwatch Secure Network analytics tool. In this paper, the DDoS attack in the Smart Grid communication networks was modeled using Stealthwatch tool. The simulated network consisted of Secure Network Analytic tools virtual machines (VMs), electrical Grid network communication topology, attackers and Target VMs. Finally, the experiments and simulations were performed, and the research results showed that Stealthwatch analytic tool is very effective in detecting and mitigating DDoS attacks in the Smart Grid System without causing any blackout or shutdown of any internal systems as compared to other tools such as GNS3, NeSSi2, NISST Framework, OMNeT++, INET Framework, ReaSE, NS2, NS3, M5 Simulator, OPNET, PLC & TIA Portal management Software which do not have the capability to do so. Also, using Stealthwatch tool to create a security baseline for Smart Grid environment, contributes to risk mitigation and sound security hygiene.

**Keywords**

Smart Grid System, Distributed Denial of Service (DDoS) Attack, Intrusion Detection and Prevention Systems, Detection, Mitigation and Stealthwatch

## 1. Introduction

### Smart Grid Background

The advancement in the Smart Grid technology has culminated in the integration of communication and computer network for Grid system-wide collection of power usage information, local energy consumption, and other measured data [1]. This development of the Smart Grid has introduced new cyber-security challenges and is a very concerning issue because of cyber-threats and security incidents that have targeted critical infrastructures all over the world. Securing the Smart Grid has become necessary due to constant cyber-attacks leading to blackout and loss of intellectual properties. Research shows that one of the crucial part of the Smart Grid infrastructure is its integral communication system [2]. A high amount of crucial data flows through the communication and computer network of the Smart Grid. Therefore, it is very important to provide a secure and reliable Smart Grid system [3]. To increase grid resilience and reliability, networked microgrids are being investigated as a promising solution. Networked microgrids are clusters of geographically close, islanded microgrids that can function as a single, aggregate island. This flexibility enables customer-level resilience and reliability improvements during extreme event outages and reduces utility costs during normal grid operations [4].

To achieve this cohesive operation, microgrid controllers and external connections (including advanced communication protocols, protocol translators, and/or internet connection) are needed. However, these advancements also increase the vulnerability landscape of networked microgrids, and significant consequences could arise during networked operation, increasing cascading impact.

**1) Problem Statement**

The Smart Grid system is an intelligent grid designed to handle surge loading and distributed generation using information and communication technology employing smart meters and control system. Because Smart Grid is embedded into open communication infrastructures to support vast amounts of data exchange, Smart Grids are vulnerable to cyber-attacks. Cyberattacks on Smart Grid include the breaching of sensitive customer data by adversaries, malware propagation, malfunctions in cyber systems, and vulnerabilities in distributed control devices. The threats could target the generation, transmission, distribution, and consumers.

Recently, the issue of Distributed Denial of Service (DDoS) attacks on the Electric grid system has been very rampant across the world. Lots of tangible assets and intellectual properties and many hours have been lost in this regard.

Additionally, attackers can make power system unstable by designing DDoS attack sequences through jamming the communication channels, attacking networking protocols, and flooding the network traffics.

Below are some of the situations of the former researchers and the problems that existed in them.

- Asri, S., Pranggono, B. Impact of Distributed Denial of Service Attack on Advanced Metering Infrastructure. Wireless Personal Communications 83(3), 2211-2223 (2015).

**Limitations**: The research was conducted using NeSSi 2 Tool and the results showed that the entire grid could be compromised with a large-enough DDoS attack but Only after the server had been taken offline was an impact observed.

- Fang *et al.* The contributions of cloud technologies to Smart Grid. Renewable and Sustainable Energy Reviews, Vol. 59, pp. 1326-1331, June (2016). The results showed the review of application of different areas of cloud computing technology in Smart Grid and finally, cloud security is briefly investigated.
- **Limitations**: No precise framework or Tool has been proposed or used to enhance the security of the Smart Grid and issues were surveyed generally.
- Abdul Rahman *et al.* Smart Grid security challenges: Classification by sources of threat. Journal of Electrical Systems and Information Technology, Vol. 5, No. 3, pp. 468-483, Dec. (2018). The authors examined security challenges of Smart Grid and they classified and analyzed identified challenges based on threat sources carefully.

**Limitations**: The proposed framework NIST is very general and vague and needs to be focused on particular domains of Smart Grid. In fact, the authors did not provide a specific solution and technique.

- Sgouras *et al.* Cyber Attack Impact on Critical Smart Grid Infrastructures. ISGT pp. 1-5. IEEE (2014). The authors considered four different types of AMI DoS setups. The results showed that DoS attack against the server caused a drop in the number of TCP packets delivered to smart meters, leading to some service degradation.

**Limitations**: The research was conducted using OMNeT++ Tool and the results showed that DDoS attack on the server reportedly diminished connections with almost 90% of the smart meters.

- Yilmaz *et al.* Cyber Security 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). pp. 81-85. IEEE (2018). The authors explored the possibility of DoS attacks against PLCs, suggesting that a PLC can be targeted both from within and outside of its own IP network, as long as its IP address is known.

**Limitations**: The research was conducted using PLC and TIA Portal Management Software Tools and the results showed that the network was quickly disrupted even with a small number of attackers.

- S. Premkumar. and V. Saminadan., "Impact of Denial of Service (DOS) attck

i Smart Distribution Grid Communication Network," *International Journal of Applied Engineering Research,* vol. 12, no. 4, pp. 4443-4447, 2017.

**Limitations**: The research was conducted using GNS3 Tool and the simulation results from the tool clearly show the vulnerability of DDoS attack in a Smart Grid power System. The destination server became overwhelmed, unavailable and shut down after consistent flooding. This was because there was no proper and reliable tool or control in place to detect, monitor and mitigate DDoS attack in place.

**2) Purpose of this Research**

The purpose and objective of this research is to detect and mitigate the Distributed Denial of Service [DDoS] attack with application to the Electrical Smart Grid System by deploying an optimized Stealthwatch Secure Network analytics tool. Stealthwatch analytic tool also has the capability to detect malware/attack in encrypted traffic without any decryption using "Encrypted Traffic Analytics [ETA]" capability on the tool. It focuses on the study of the practical ways to detect and mitigate DDoS attacks when data are transferred over Smart Grid Communication Networks without any adverse effect on the internal systems or any shutdown of the systems due to attack.

Unfortunately, no technology today can completely keep hackers out of enterprise networks. However, if an organization is regularly monitoring its own environment with the right mix of people, processes and technology, the security team will be better equipped to identify and stop an attack while it's still happening, avoiding the disastrous results and costs associated with a data breach.

## 2. Literature Review

### Introduction

The Smart Grid is the modern system of wires, meters, and transformers that work together to power our homes and businesses. We connect ourselves to the Smart Grid when we plug in our devices and click on the light switch. The electricity grid is older than you might have thought—it was developed in the 1890s and evolved along with our ever-changing technology [5]. Today, the modern Smart Grid contains over nine thousand electricity generating units, has over one million megawatts of generating capacity, and is connected to more than three hundred thousand transmission lines. Smart Grid is divided into three main networks: the operation network, the business network, and the customer network. Each of these three networks has individual set of communication subnetworks serving different functions. The first, operation network is used for maintaining the Grid functionality by the power companies. The second one, the business network is used by the participants in the electricity market to effectively regulate the market and to provide electricity services to the customers at large. The last part which is the customer network is used by individual customer for management of their home energy and to enhance the electricity usage [6]. Due to the division of the Smart Grid networks in terms of communication,

Smart Grid is divided into three areas as shown in Figure 1. such as WAN, HAN, and NAN. WAN (Wide Area Network) provides communication links or interface between the NANs and the utility systems in order to transfer information. NAN (Neighborhood Area Network) in its case connects multiple HANs to the local access points. HAN (Home Area Network), this communication is for end user home or business communications [7].

Figure 2 below depicts generic Smart Grid Network Architecture components or modules with different reference points.

As shown, typical Smart Grid network consists of following components.

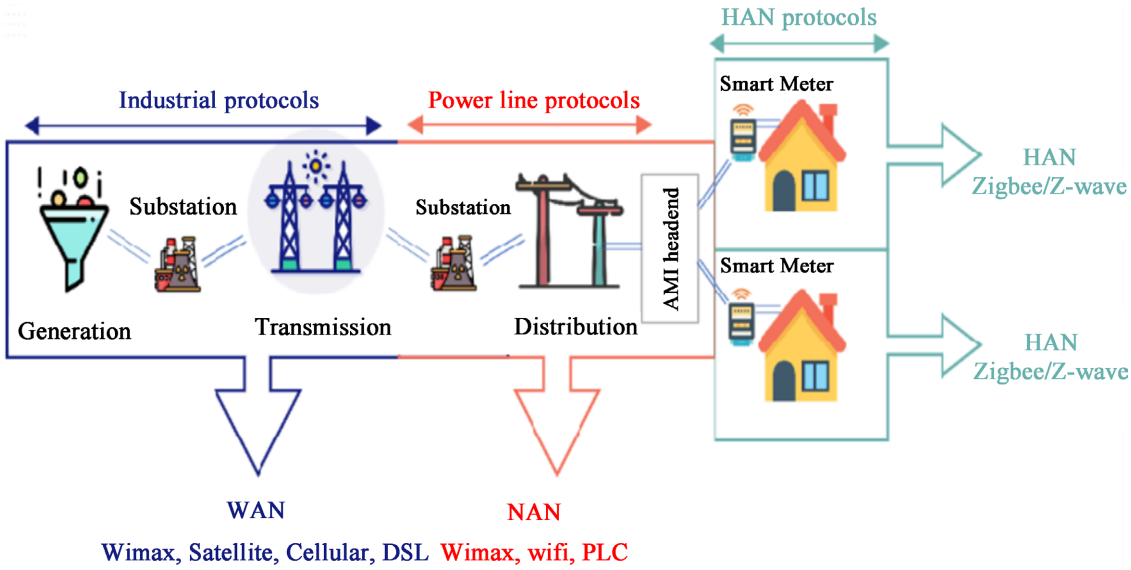



Figure 1. Illustration of Smart Grid network architecture [7].

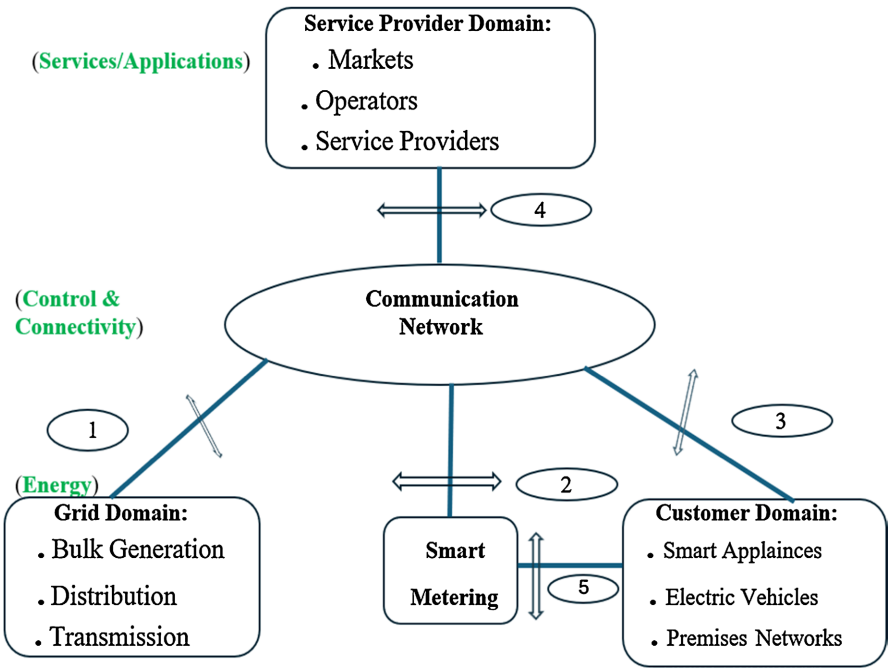



Figure 2. Generic Smart Grid Network Architecture components [8].

Grid domain: Operations include bulk generation, distribution, and transmission Smart meters Consumer domain: HAN (Home Area Network) consists of smart appliances and more. Communication network: This connects smart meters with consumers and electricity company for energy monitoring and control operations, include various wireless technologies such as Zigbee, wifi, HomePlug, cellular, GSM, GPRS, 3G, 4G-LTE, etc. Third-party service providers: system vendors, operators, web companies etc.

Smart Grid security has attracted a lot of attentions from both academic and industry communities. Some of the reviews and comments are thereby highlighted as part of this research paper. Asri, S., Pranggono, B. Impact of Distributed Denial of Service Attack on Advanced Metering Infrastructure. Wireless Personal Communications 83(3), 2211-2223 (2015) [3]. The results showed that the entire grid could be compromised with a large-enough DDoS attack but Only after the server had been taken offline was an impact observed. Fang *et al*. The contributions of cloud technologies to Smart Grid. Renewable and Sustainable Energy Reviews, Vol. 59, pp. 1326-1331, June (2016) [9]. The results showed the review of application of different areas of cloud computing technology in Smart Grid and finally, cloud security is briefly investigated. No precise framework has been proposed to enhance the security of the Smart Grid and issues were surveyed generally. Abdul Rahman *et al*. Smart Grid security challenges: Classification by sources of threat. Journal of Electrical Systems and Information Technology, Vol. 5, No. 3, pp. 468-483, Dec. (2018) [10]. The authors examined security challenges of Smart Grid and they classified and analyzed identified challenges based on threat sources carefully. Meanwhile, their proposed framework is very general and vague and needs to be focused on domains of Smart Grid. In fact, the authors did not provide a specific solution and technique. Shrestha. M *et al*. A Methodology for Security Classification applied to Smart Grid Infrastructures. International Journal of Critical Infrastructure Protection, 28 (2020) [11]. The authors proposed a methodology called Smart Grid Security Classification (SGSC) developed for complex systems such as the Smart Grid. They indeed covered risk analysis methods, security criteria and protection mechanism in their methodology. Their methodology does not support automatic computation of scores and multi-metrics approach. K. Demir *et al*. Securing the cloud-assisted Smart Grid. International Journal of Critical Infrastructure Protection, pp. 100-111, Dec. (2018) [12]. The authors proposed cloud computing technology to improve the security of the Smart Grid. They specifically concentrated on distributed denial of service attack and counteracting it. There is no comprehensive approach to enhance Smart Grid security using cloud computing technology in this paper and it focuses only on countering a specific attack. Souris, K.I *et al*. Cyber Attack Impact on Critical Smart Grid Infrastructures. ISGT pp. 1-5. IEEE (2014) [5]. The authors considered four different types of AMI DoS setups. The results showed that DoS attack against the server caused a drop in the number of TCP packets delivered to smart meters, leading to some service degradation. Al-

so, the DDoS attack on the server reportedly diminished connections with almost 90% of the smart meters. Yilmaz, E.N *et al.* Cyber Security 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). pp. 81-85. IEEE (2018) [13]. The authors explored the possibility of DoS attacks against PLCs, suggesting that a PLC can be targeted both from within and outside of its own IP network, as long as its IP address is known. The results showed that the network was quickly disrupted even with a small number of attackers.

In reality, Smart Grid is divided into three main networks: operation, business, and customer networks. Each of these three networks has an individual set of communication subnetworks serving different functions. First, the operation network is used for maintaining the Grid functionality by the power companies. The second one, the business network, is used by the participants in the electricity market to regulate the market effectively and provide electricity services to the customers at large. The last part, the customer network, is used by the individual customers to manage their home energy to enhance electricity usage [3]. Due to the division of the Smart Grid networks in terms of communication, Smart Grid is divided into three areas: WAN, HAN, and NAN. WAN (Wide Area Network) provides communication links or interfaces between the NANs and the utility systems to transfer information. In its case, NAN (Neighborhood Area Network) connects multiple Hans to the local access points. In the case of HAN (Home Area Network), this communication is for end-user home or business communications [4].

## 3. Cyber Security Threat in Smart Grid System

### Cyber Threats to the Smart Grid

Attacks against the Smart Grid will likely differ from many traditional attacks against cyber environments. First, an attacker must be able to compromise the grid's cyber elements. However, for the attack to cause negative system impact, the attacker must also know how to control the cyber elements in order to manipulate the physical system. **Figure 3** demonstrates this relationship.

In the Smart Grid, the most severe threats related to the privacy deterioration of Smart Grid consumers include [15] [16].

- Intrusion and cyber-attack: This occurs when an attacker uses stolen credentials, phishing attacks, or other means to gain access to your system.
- Identity theft: This occurs by using sophisticated cyber-attack tactics, including social engineering, phishing, and malware to steal.
- Loss of intellectual property: IP theft can refer to someone stealing patents, copyrights, trademarks, or trade secrets. This includes names, logos, symbols, inventions, client lists, and more.
- Observing the behavioral attitude of the consumers and the appliances that they used: Attackers uses this to attack their end users.
- Consumers' lack of awareness: The customers need to learn adequately about

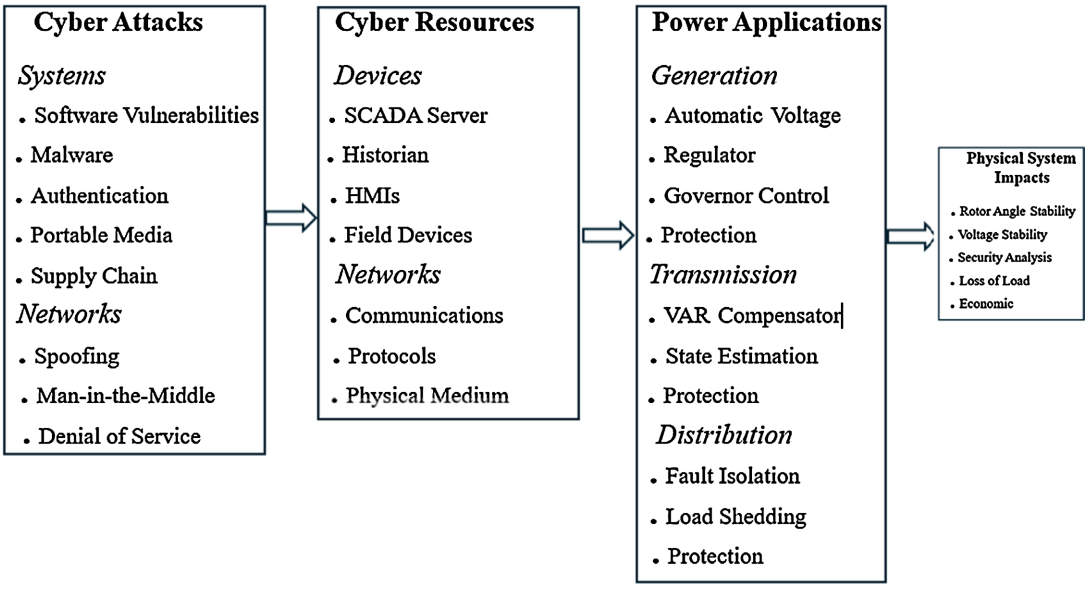



**Figure 3.** Attacks to the Smart Grid [14].

the risks, costs, and advantages of the SG systems, because of the demand for a higher level of security.

- Young and unknown technologies: Many new technologies are adding to the Smart Grid and could be eye-catching to hackers to easily explore point of weaknesses.
- Scalability: The growth in the quantity of circulating data and energy flows, the SG protocols, and the size of network structure directly affect the size and complexity of the SGs. This volume of information and complexity might cause data accumulation, and control efficiency destruction, if not handled and accommodated properly in the SG.
- The weakness received from joined communication technologies: Applying existing ICTs in the structure of the SGs can lead to inheriting all the vulnerabilities and problems from these technologies to the SG system.
- Lack of standards and regulations: To achieve interoperability, standards and regulations must include each part of the SG.
- Man-in-the-Middle attack: Eavesdropping on the SG communication network can make hacker to have unauthorized access to the SG.
- Distributed denial of service attack (DDoS): A DDoS attack can lead to power shutdown and degradation of service.
- False data injection attack: False data injection attack is able to have an impact on the operation and control of SGs by passing the bad data detection systems by compromising sensors and made to mimic the events that do not occur at all.

**How Does Attack Happen in the Environments: The Seven Kill Chains**

The cyber kill chain (CKC) is a classic cybersecurity model that is developed to better understand the stages an attack must go through to conduct an attack and help security teams stop an attack at each stage [17]. **Figure 4** below shows the seven steps in the kill chain.

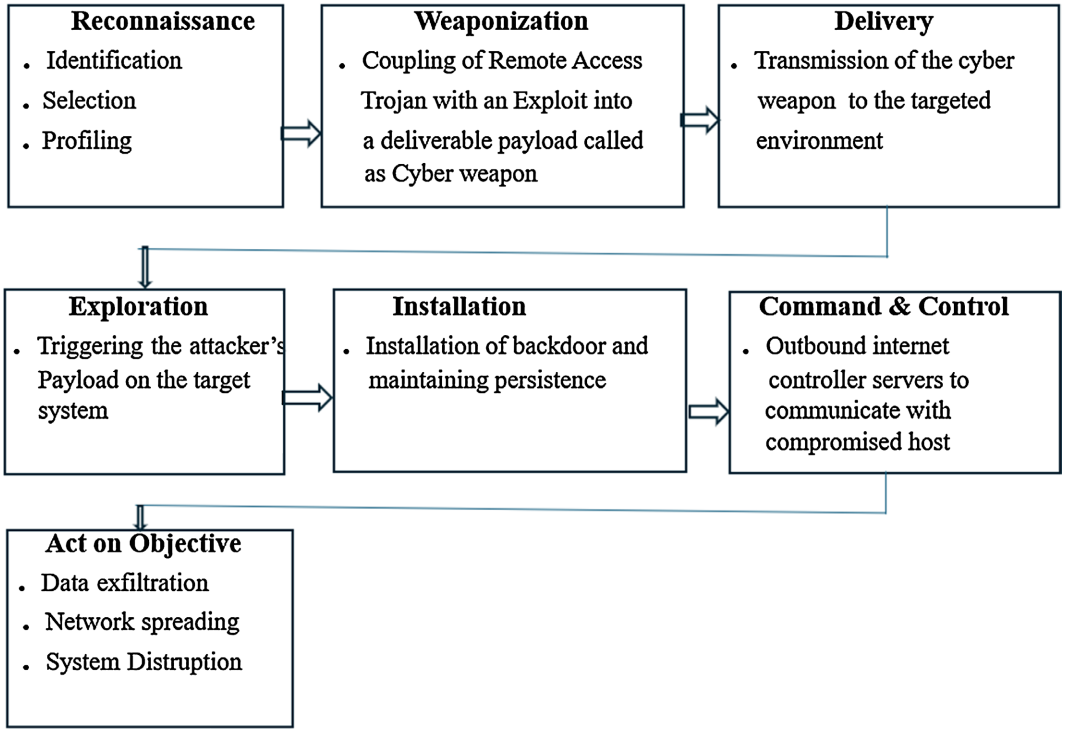



**Figure 4.** The seven kill chains [17].

## 4. Methodology

### Materials and Methodology

In this section, the tools/devices/materials, codes, algorithms, and Lab apparatus simulation techniques used for the Detection and Mitigation of Distributed Denial of Service (DDoS) attack in application to Smart Grid System have been discussed in detail.

**1) The Materials, Devices and Tools**

In this research, the strategy started by building the Flow Collector virtual machine (VM), Flow Sensor virtual machine (VM) and Stealthwatch management console virtual machine (VM) and then assigned IP addresses in accordance with the simulated communication Network designed model as shown in Figure 5. The flow rate licenses is also one of the required components when deploying Stealthwatch analytics tool. Also, the attackers/source virtual machine (VM) and Target/destination virtual machine (VM) have also been built and assigned IP addresses per the simulated communication Network as well, and both can send and receive icmp/ping packets with no issues. The traffic between the attacker's system and the target server has also been captured on the Stealthwatch management console under normal or baseline operation. The model setup already validated that traffic can go from attacker's system to the target server and is captured on our Stealthwatch management console and thin client with no issues. We later then Installed or ingested DDoS payload/malicious codes on the attacker's machine to carry out the DDoS operations on the target

server/machine so that our model Stealthwatch tools can capture, detect, and mitigate the DDoS attack without any impact on the target system. In the simulation, once the flow level rises above the defined baseline on the target system based on our coding/algorithm, this will generate an alert to the administrator to take proper action before it affects the target server.

**2) The Secure Network Analytics Components**

Figure 5 below shows the materials samples of Secure Stealthwatch Analytics components used in this research to detect and mitigate DDoS attack in Smart Grid system.

| Manager | Flow Collector | Flor Sensor |
|---|---|---|
|  <br>SMC VE (Virtual Edition)<br>SMC 2210<br>• SMC for Management & Configuration supports.<br>• Up to 25 Flow Collectors<br>• 10000 Network access user Sessions<br>• 15 concurrent managing users<br>• Scale up to 6 Million FPS in one deployment |  <br>Flow Collector VE<br>FC 4210/FC 5210<br>• Flow Collector in the center of Data Collection and analytics<br>• Up to 25 FC per deployment<br>• Up to 240,000 FPS per FC<br>• Up to 6TB of flow storage<br>• Up to 1 Million Host Classified<br>• Up to 4000 Data Source per FC |  <br>Flow Sensor VE<br>FS 1210/ FS 3210/ FS 4210<br>• Ingest SPAN to generate telementry and contextual data<br>• Up to 80Gbps per FS, Coper and Fiber supported interface<br>• 1Gb, 10Gb and 40Gb monitor interfaces |

Figure 5. Secure Stealthwatch network analytics components [18].

**3) Stealthwatch Analytics Tools Build**

**Flow Collector Build**

Figure 6 below shows the process or steps used to build the flow collector used in this research.

After the VM has been assigned.

Step 1: Entering the configuration mode in the network option.

Step 2: Figure 7 below shows the steps to configure FC the IP address/hostname details as shown below:

IP address====192.168.232.206

Subnet Mask==255.255.255.192/6

Gateway=====192.168.232.193

Broadcast Address==192.168.232.225

Hostname========fm2lab-sw-fc01

**Flow Senosr Build**

Figure 8 below the process or steps used to build the flow sensor used in this research.

After the VM has been assigned:

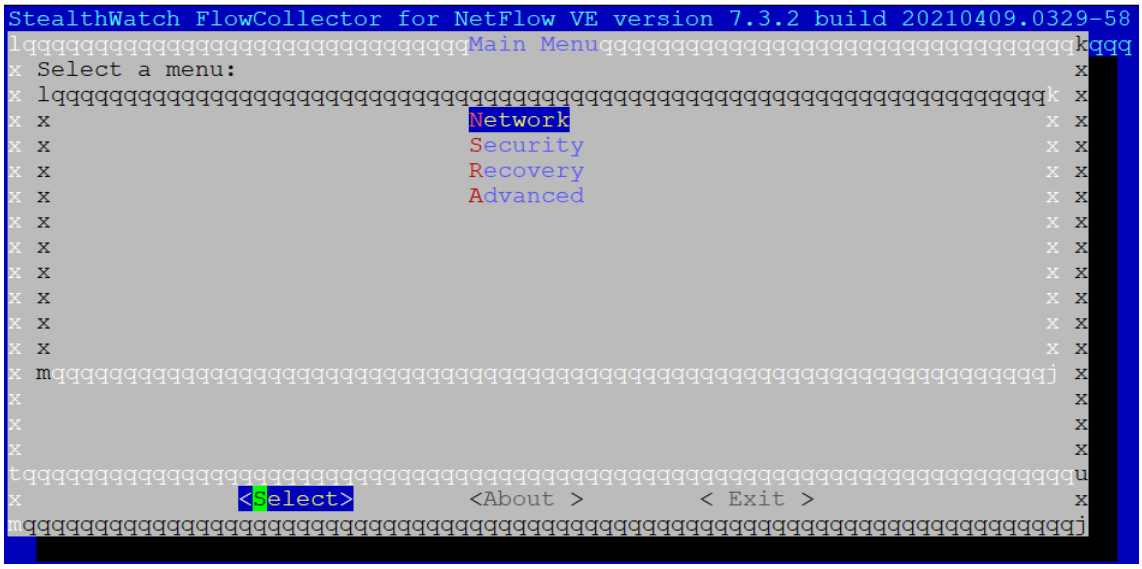



Figure 6. Flow collector build interface.

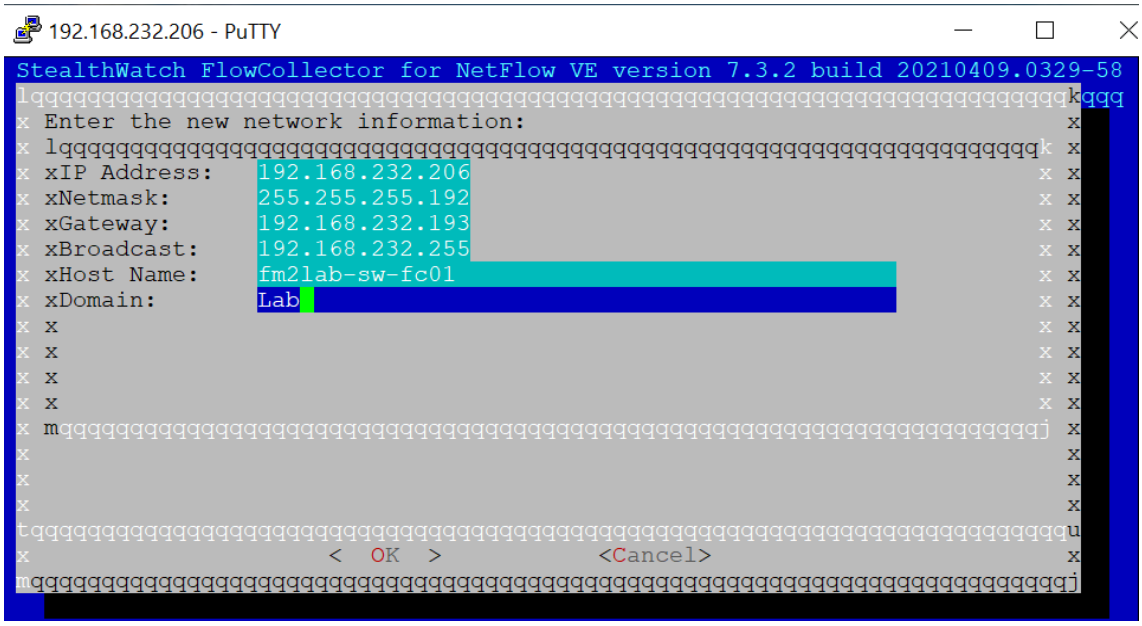



Figure 7. Flow collector build network interface settings.

Step 1: Entering the configuration mode in the Network option.

Step 2: Figure 9 below show the steps to configure FS the IP address/hostname details as shown below:

IP address====192.168.232.207

Subnet Mask==255.255.255.192/6

Gateway=====192.168.232.193

Broadcast Address==192.168.232.225

Hostname========fm2lab-sw-fs01

**Stealthwatch Management Console Build**

Figure 10 below shows the process or steps used to build the Stealthwatch

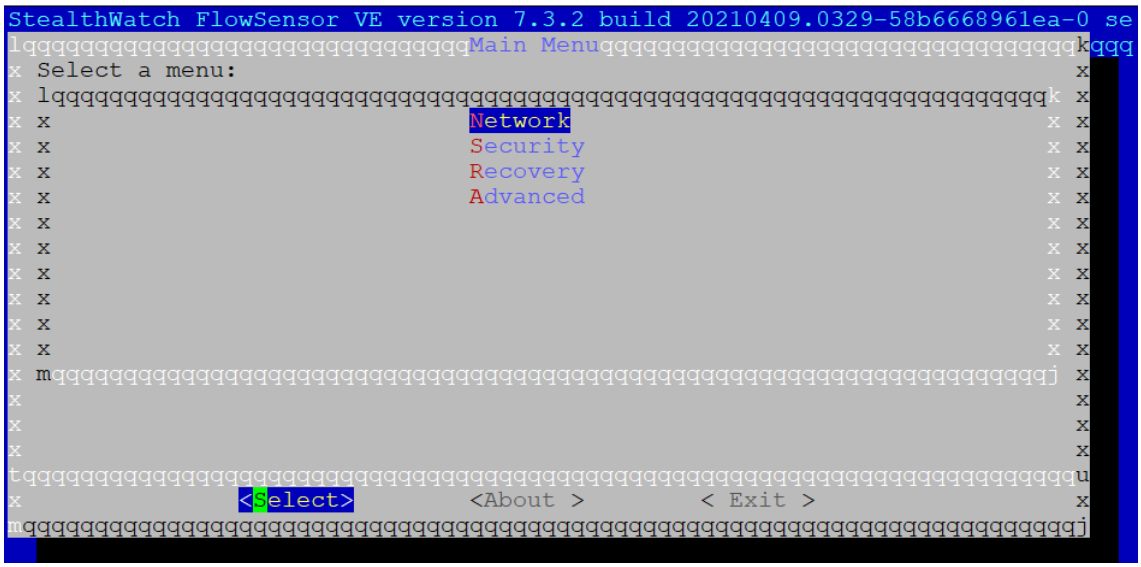



**Figure 8.** Flow sensor build interface.

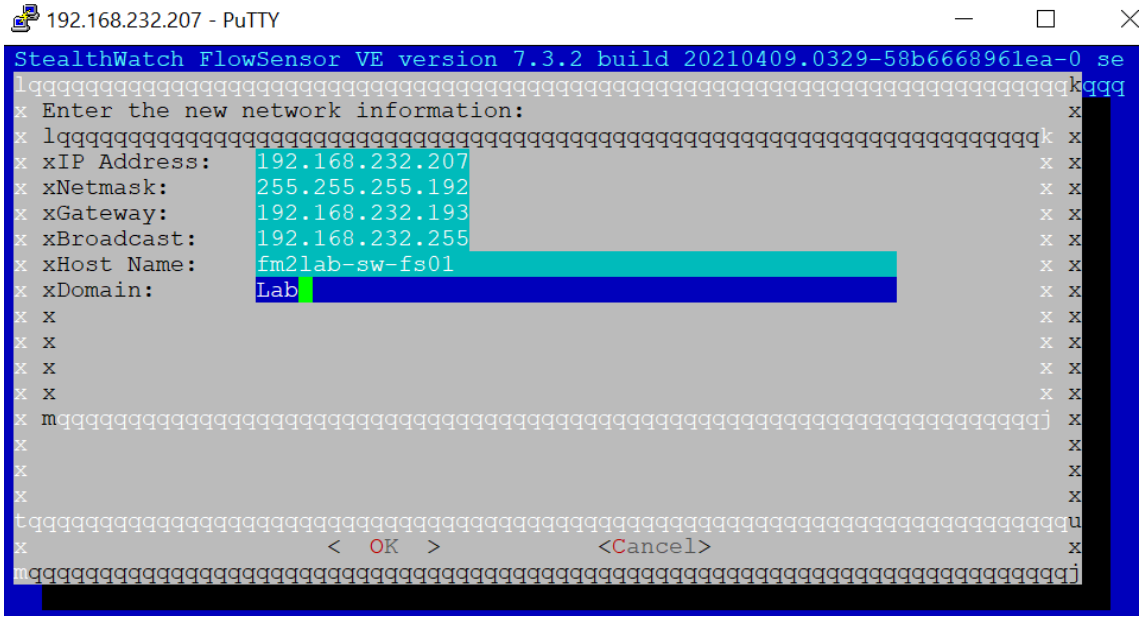



**Figure 9.** Flow sensor build network interface settings.

Management Console used in this research.

After the VM has been assigned:

Step 1: Entering the configuration mode in the Network option.

Step 2: **Figure 11** below show the steps to configure Stealthwatch Management Console IP address/hostname details as shown below:

IP address====192.168.232.205

Subnet Mask==255.255.255.192/6

Gateway=====192.168.232.193

Broadcast Address==192.168.232.225

Hostname========fm2lab-sw-fs01

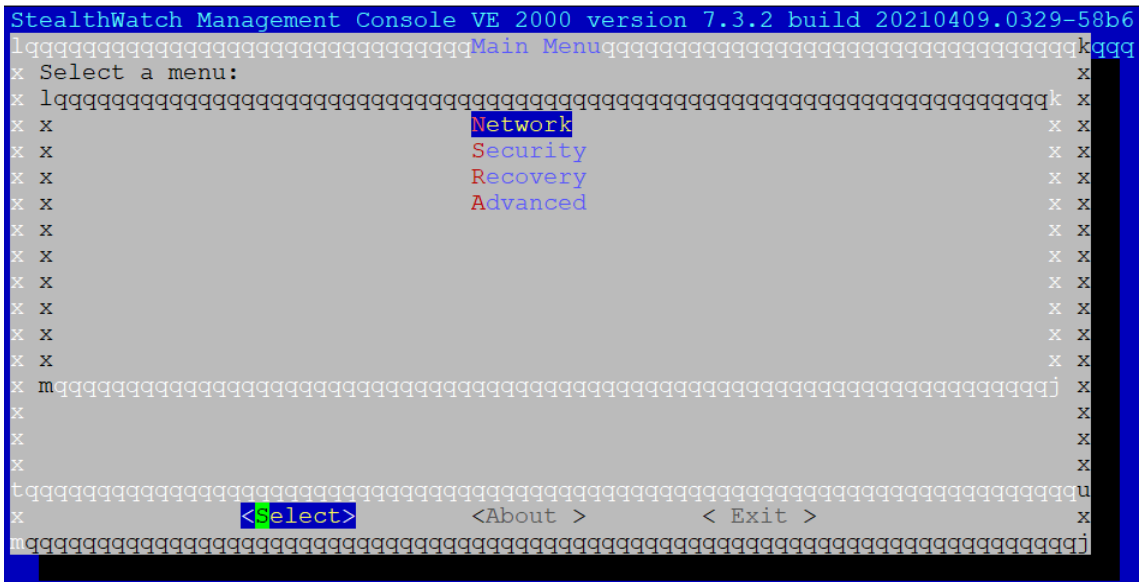



Figure 10. SMC build interface.

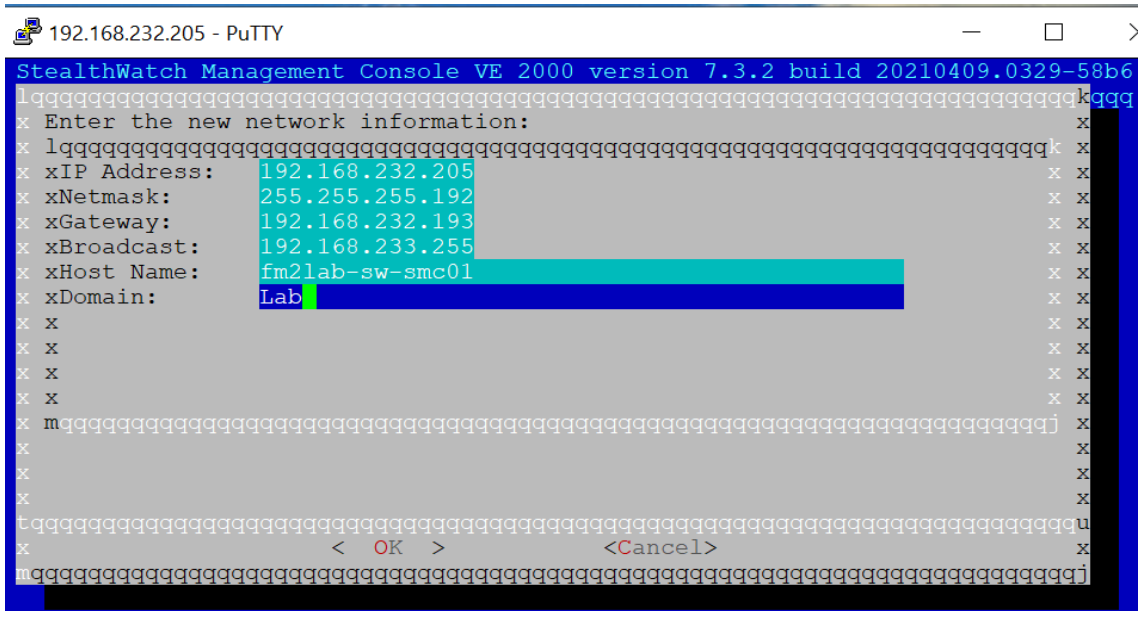



Figure 11. SMC build network interface settings.

**Attacker-Source Host1 Build**

Figure 12 below is the set-up build for the attacker's/Host1 VM used in this research. After the VM has been assigned:

Step 1: The IP addresses configurations info:

IP Address==192.168.232.209

Subnet Mask==255.255.255.192

Gateway=====192.168.232.193

Broadcast Address===192.168.232.255

Hostname========fm2lab-nsm

Step 2: System build

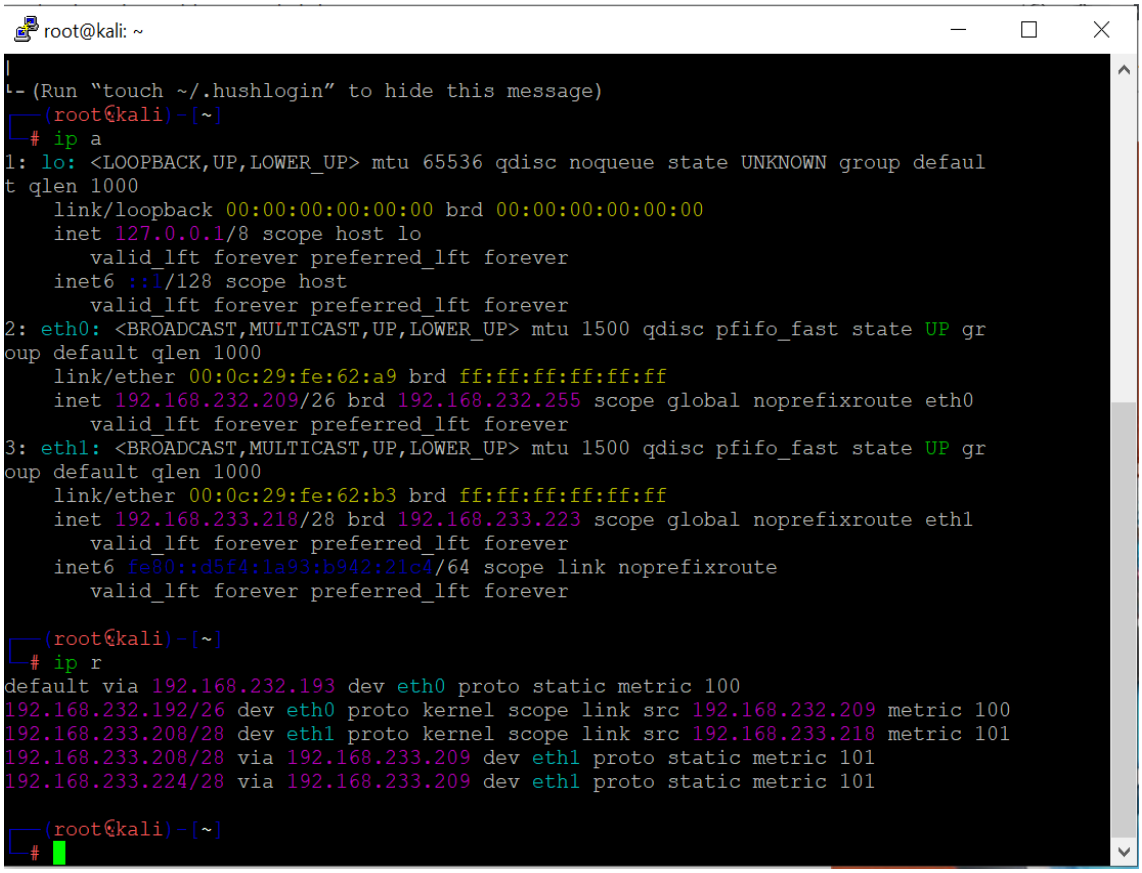



Figure 12. Attacker [Host1] VM build.

**Target-Destination Host2 Build**

Figure 13 below is the set-up build for the attacker's/Host1 VM used in this research. After the VM has been assigned:

Step 1: The IP addresses configurations info:

IP Address==192.168.233.214

Subnet Mask==255.255.255.240

Gateway=====192.168.233.209

Broadcast Address===192.168.233.223

Hostname========ubuntu214

Step 2: System build

**4) Proposed Design Using Stealthwatch Tools**

**Scenario Formation/Simulation Process**

Figure 14 shows the Proposed Networked Smart Grid and its Communication Computer Network Design Using Stealthwatch which we considered in this research. In this network, we have chosen Host1 (192.168.232.209) as source and Host2 (192.168.233.214) as destination which is connected to Router R3 and R9. The routers R1 and R9 come under the Customer Edge networks.

Here, both Host1 and Host2 are connected to virtual machine which is created by VMWare. All other routers are coming under ISP Router. After creating the network, addresses were assigned as shown in the figure below. Here we choose

```
root@Ubuntu212: ~
login as: sgadmin
sgadmin@192.168.233.214's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Sep 14 08:15:52 PDT 2022

  System load:  0.06              Processes:           81
  Usage of /:   24.8% of 14.38GB  Users logged in:     0
  Memory usage: 9%                IP address for eth0: 192.168.233.214
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

166 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 14 08:15:52 2022
sgadmin@Ubuntu212:~$ sudo su -
[sudo] password for sgadmin:
root@Ubuntu212:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 00:0c:29:fd:fc:da brd ff:ff:ff:ff:ff:ff
    inet 192.168.233.214/28 brd 192.168.233.223 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefd:fcda/64 scope link
       valid_lft forever preferred_lft forever
root@Ubuntu212:~# ip r
default via 192.168.233.209 dev eth0
192.168.233.208/28 dev eth0  proto kernel  scope link  src 192.168.233.214
root@Ubuntu212:~#
```

**Figure 13.** Target server [Host2] VM build.

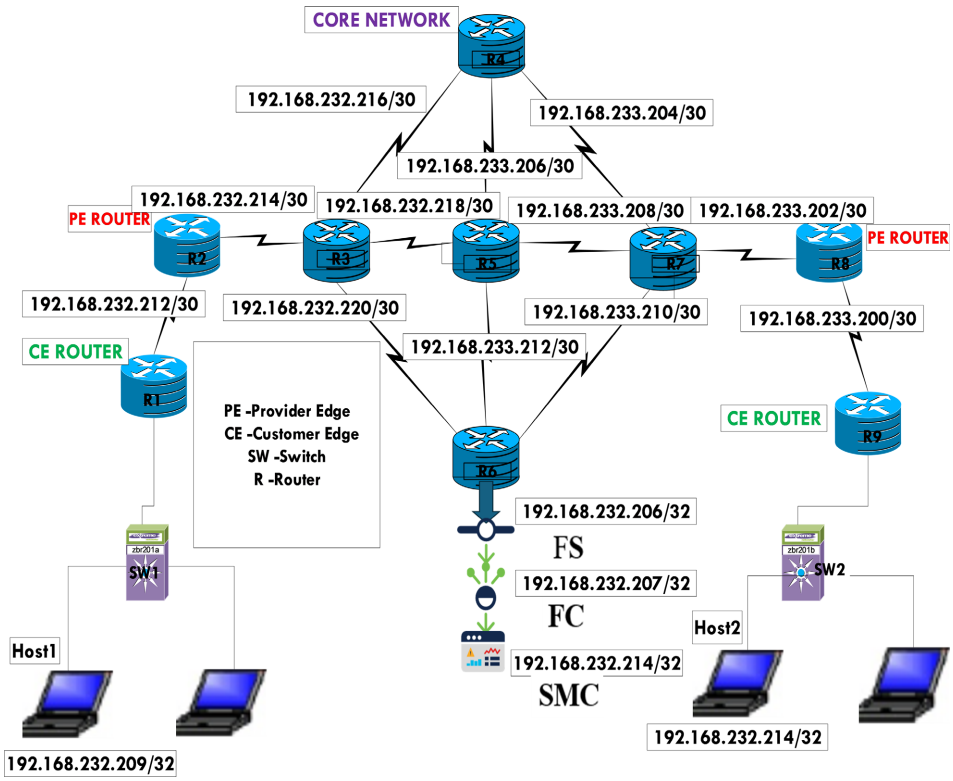
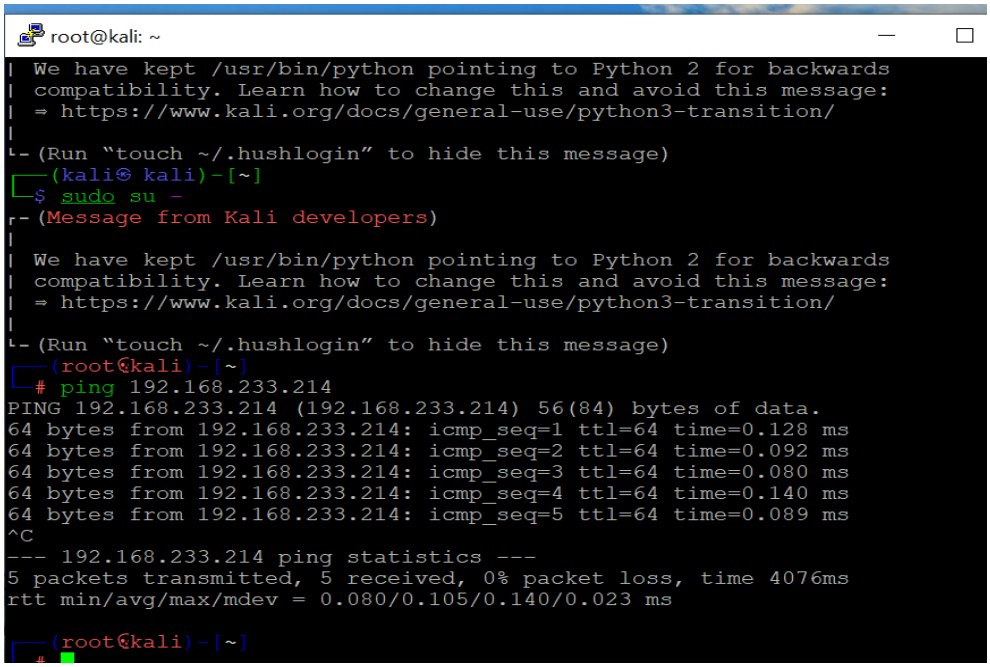


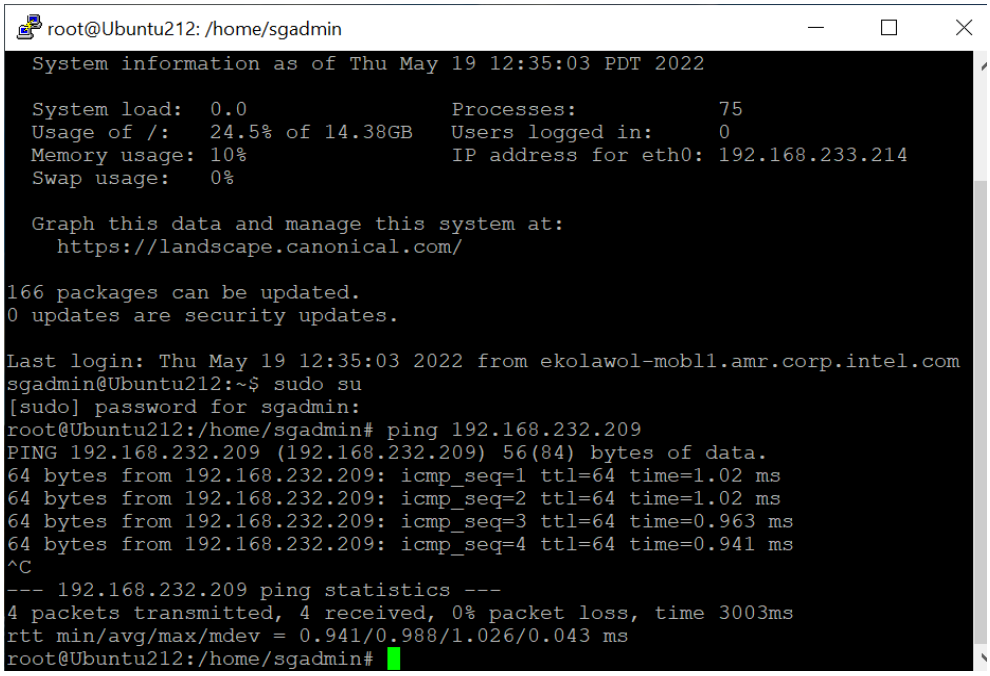

**Figure 14.** Proposed Smart Grid communication using Stealthwatch tool.

logical addressing scheme which is IP addressing and IPv4 addressing scheme is specifically used in this research which is subnetted by using VLSM to reduce the minimum wastage of IP's. All the networks of the proposed architecture use IPv4 and are all connected to the network without any issues.

Once all the VMs have been built and addressed with IP details, Figure 15(a)




(a)




(b)

**Figure 15.** (a) Ping status between attacker (Host1) and target server (Host2); (b) Ping status between target server (Host2) and attacker (Host1).

& Figure 15(b) then show the communication between the source node [attackers VM] to destination node [Target inside host] through our designed/proposed Stealthwatch network. To check the communication between the desired nodes in this research we use ping command, which works based on ICMP protocol. Based on echo request and echo reply between the source and destination we can find the communication status. Also, Figure 16 displays the ping status throughput though our Stealthwatch tool to confirm the communication success between the two VMs. The figure also validates the Stealthwatch capability to see the traffic passing the grid system.

**5) Stealthwatch Smart Grid Firewall-IPS Rules, Security Event and Flowchart**

During this research, Figure 17 below displays the firewall rule that was implemented in carrying out the research using Forcepoint next-generation Firewall.

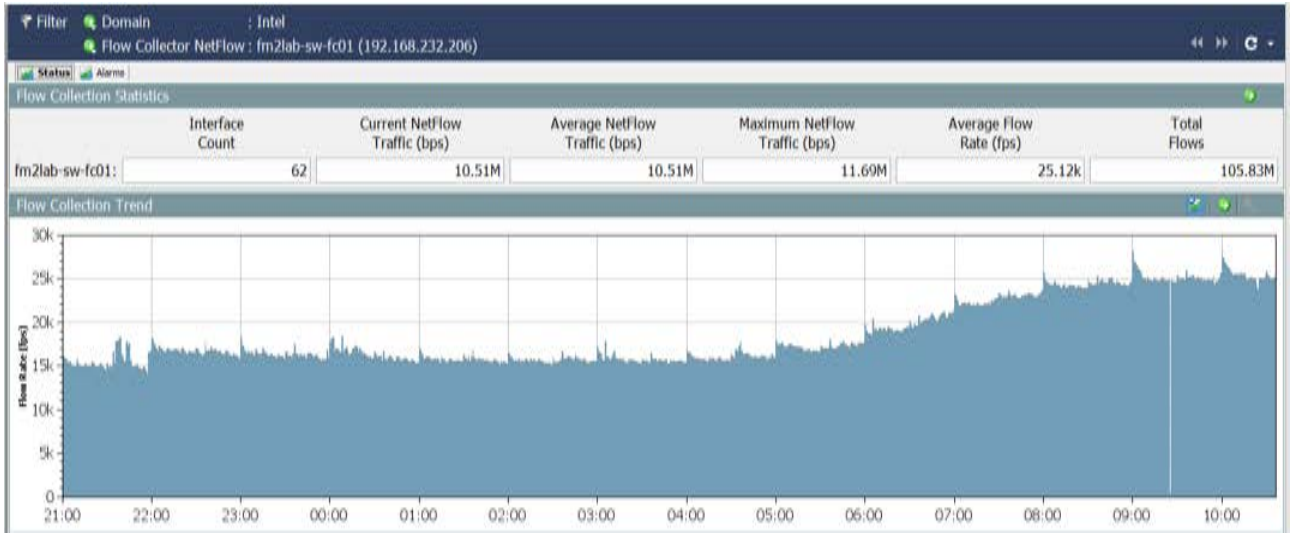



Figure 16. Flow level capture by Smart Grid computer Stealthwatch analytic tool between attacker (Host1) and target server (Host2).

| ID | Source | Destination | Service | Action | Logging | Rule Name | Comment |
|---|---|---|---|---|---|---|---|
| Stealthwatch -Smart-Grid-LAB-Rules | | | | | | | |
| 2160 | h_192.168.232.209 | host_192.168.233.214 | ANY | Allow | Stored Connection Closing: No Log | @2227354.7 | Stealthwatch -Smart-Grid-Rules |
| 2161 | host_192.168.233.214 | h_192.168.232.209 | ANY | Allow | Stored Connection Closing: No Log | @2227355.7 | Stealthwatch -Smart-Grid-Rules |
| 2162 | FM_LAB_192.168.232.0_24 | FM_LAB_192.168.233.0_24 | ANY | Allow | Stored Connection Closing: No Log | @2227352.7 | Stealthwatch -Smart-Grid-Rules |
| 2163 | FM_LAB_192.168.233.0_24 | FM_LAB_192.168.232.0_24 | ANY | Allow | Stored Connection Closing: No Log | @2228379.4 | Stealthwatch -Smart-Grid-Rules |
| 2164 | ANY | FM_LAB_192.168.232.0_24<br>FM_LAB_192.168.233.0_24 | ANY | Discard | Stored Connection Closing: No Log | @2228378.5 | Stealthwatch -Smart-Grid-Rules |

Figure 17. Proposed Stealthwatch Smart Grid firewall rules

The firewall rules displayed the access that was allowed between the attack system or source client and the target server or destination server. The default denial rule was placed at the bottom of the firewall rule as the best practice.

Figure 18 below displays the Intrusion Detection System (IPS) rules that were implemented during the course of this research for the protection and security of the entire Smart Grid system use case.

Figure 19 shows the remodified flowchart of cyber-attack algorithm using Stealthwatch. It details how Stealthwatch detects anomaly on the network and generate alerts based on the threshold volume level.

**6) Optimization/Modification of Stealthwatch Codes & Flow Data for Smart Grid System**

Figure 20 below shows the optimized/modified codes used for the implementations. The codes are used during the deployment of our Stealthwatch tool to set parameters based on baseline per traffic volume. This is a significant part of the research to detect when there is an anomaly in the Smart Grid system for immediate detection and mitigation before it affects the Grid System. It shows the baseline volume of flowrate ratio set to 15 pfs as baseline without DDoS

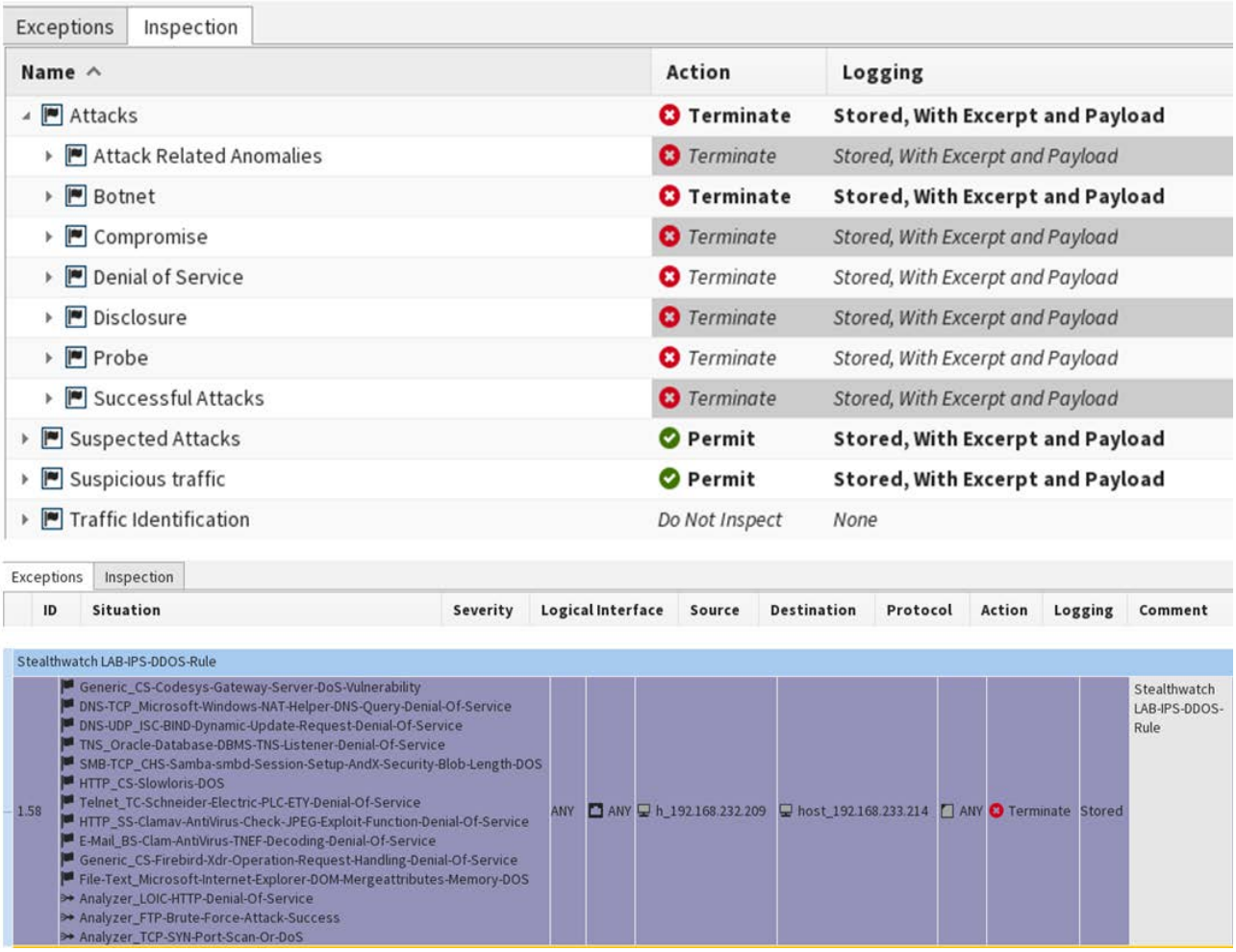



**Figure 18.** Proposed Stealthwatch Smart Grid IPS rules.

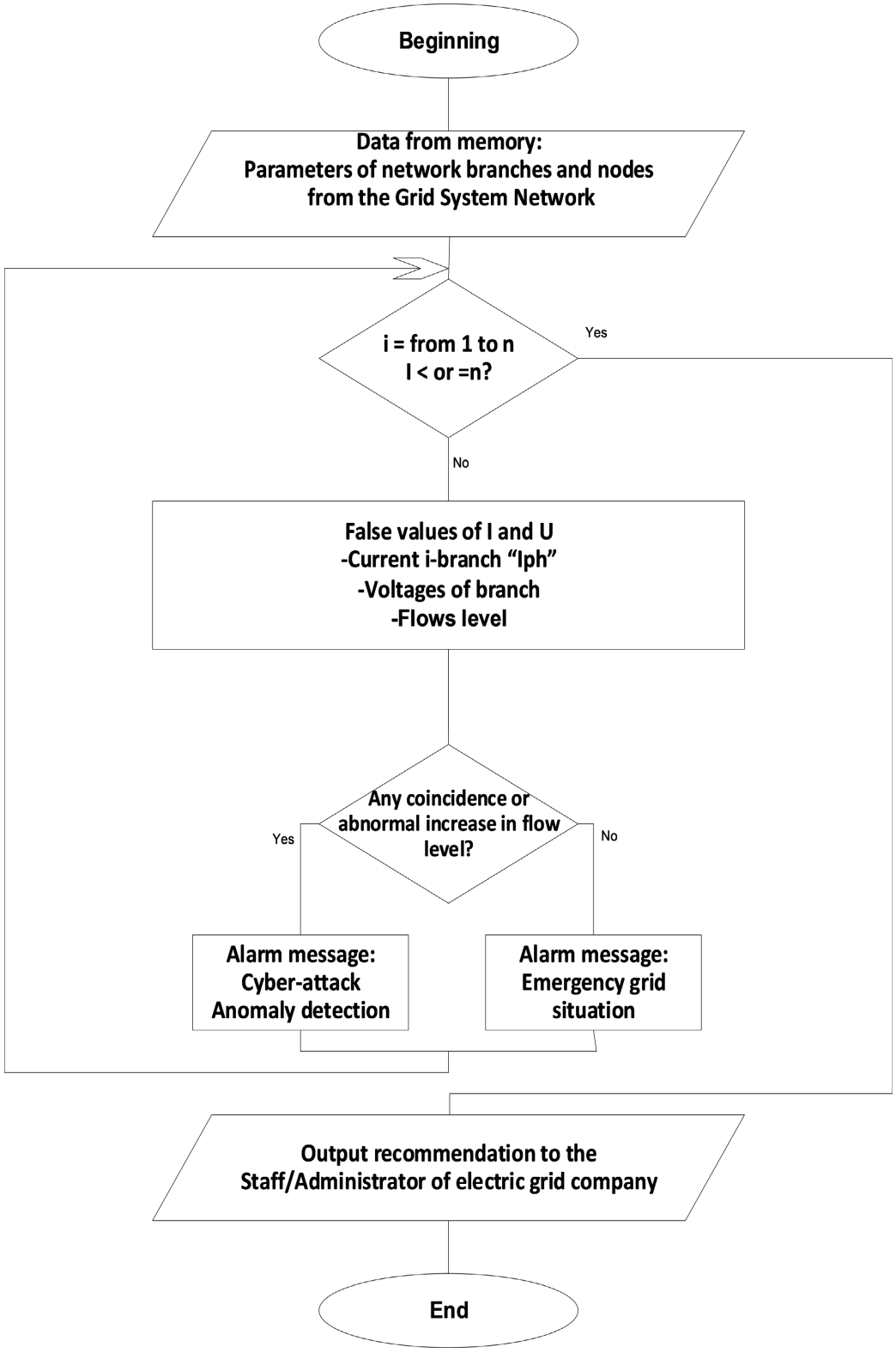



**Figure 19.** Proposed block diagram of Smart Grid cyber-attack algorithm using Stealthwatch.

attack. When the flow rate ratio goes above 15 pfs, the alert/alarm sets in before the attack occurs.

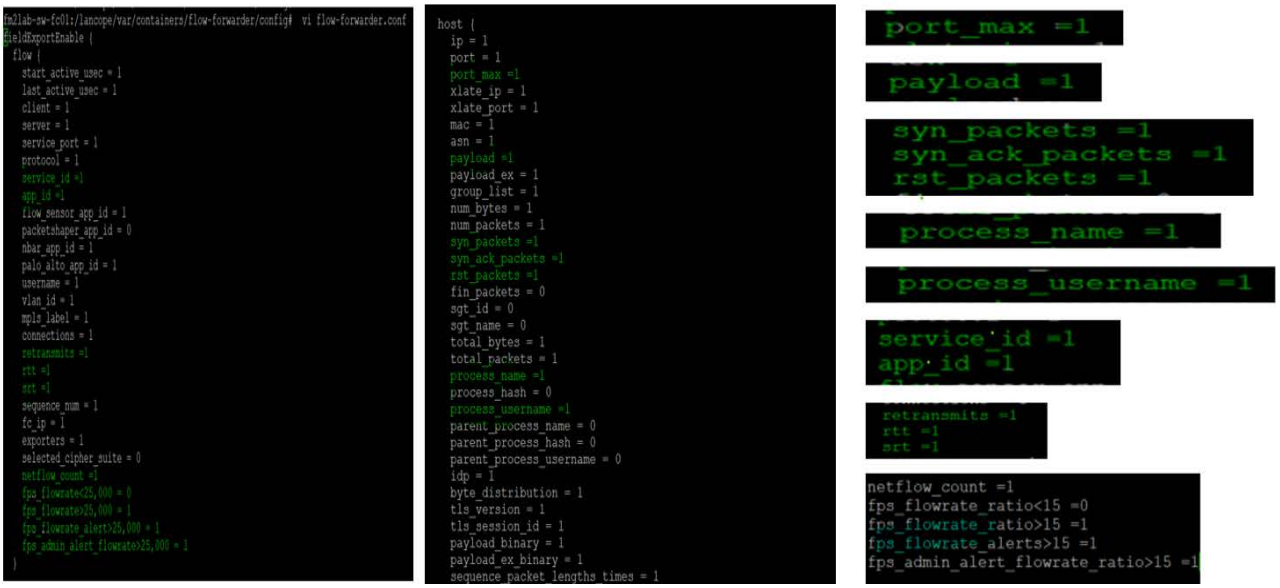
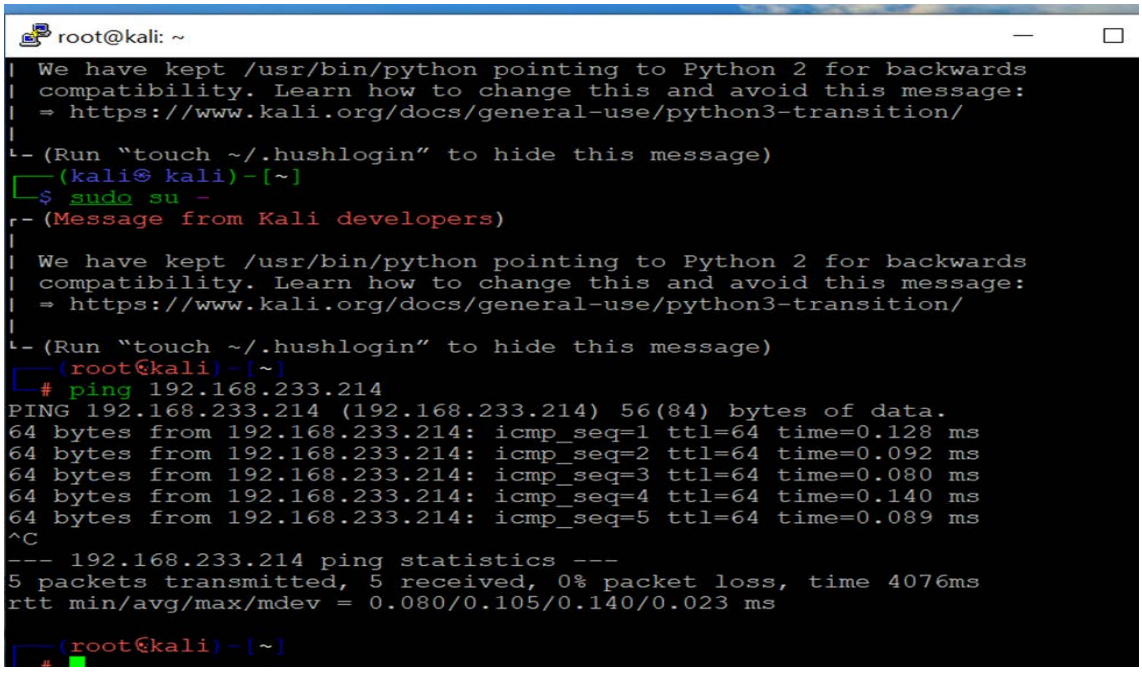



**Figure 20.** Optimized Stealtwatch coding and flow data for Smart Grid system.

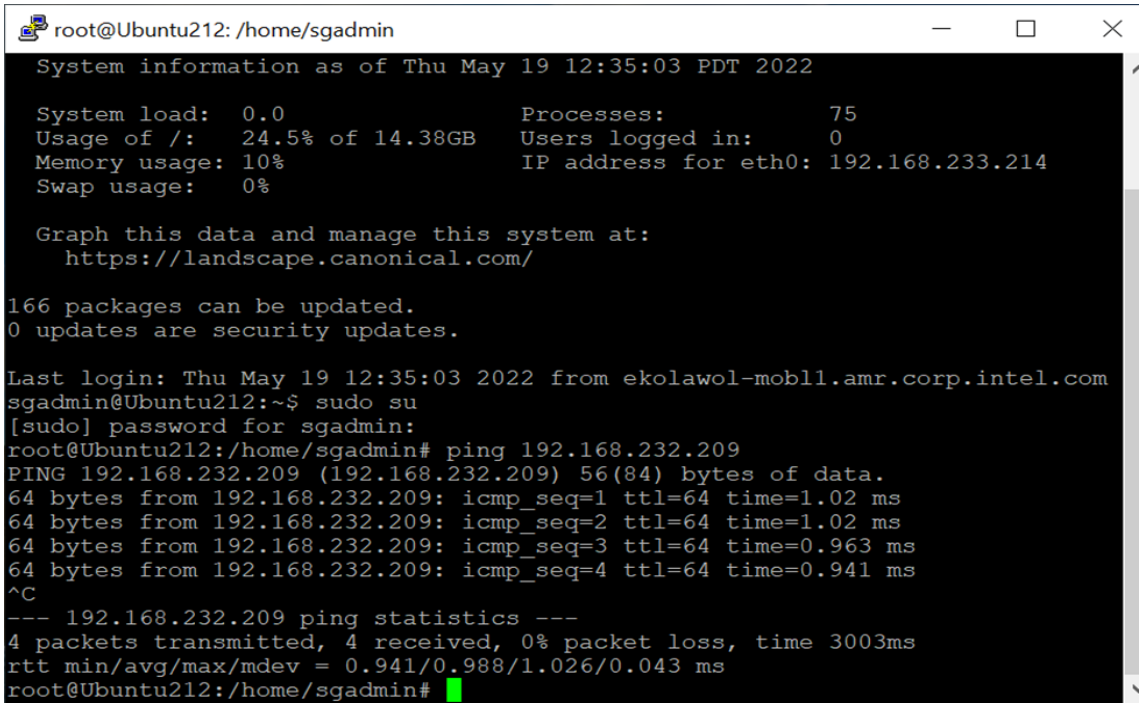
## 5. Findings

### Simulations Analysis and Results

In this section, our main concern and purpose of this simulation is to show the impact of DDoS attack in the proposed Smart Grid distribution network and how it is been detected, captured, and mitigated by our Secure Network Analytics (Stealthwatch) device/tools before it shuts down the grid completely. The data packets sent from Host1 to Host2 are captured using Stealthwatch central management console. Figure 21(a) and Figure 21(b) show the communication




(a)




(b)


(c)

**Figure 21.** (a) Ping status between Attacker (Host1) and Target Server (Host2); (b) Ping status between Attacker (Host1) and Target Server (Host2); (c) Ping status between Attacker (Host1) and Target Server (Host2) with Stealthwatch tool analytics before the attack

between the source node-Host1 (Attacker) to destination node-Host2 (Target Server) through Smart Grid Stealthwatch computer network. The figure also shows that the attacker server (Host1) with IP address 192.168.232.209 is able to reach Host2 with IP address 192.168.233.214 and vice-versa through icmp/ping protocol.

**1) Simulations Before the Attack Happened**

Figure 21(a) and Figure 21(b) show the ping status between the attacker and Target systems during the simulation phases.

Figure 21(c) below shows that Stealthwatch Analytic tool is able to capture

the communication between the attacker and the Target devices with no issues. Based on the echo request and echo reply between the source and destination, we can find the communication status.

**2) Simulations During the Attack**

Figure 22 below narrates the simulation results during and after the attack happpened. It displays the ingestion of malicious codes for DDoS attack in the attack system or source client in the form of excessive ping and port scan over 600 sockets as shown. This is to overwhelm and shut down the target or destination server. The figure also displays the Tcpdump simulation results that explain how the traffic is hitting the destination server per payload sent from the attack system. The TCPdump shows that the Attacker [Source Server-192.168.232.209] is constantly sending ping/port scans to Target [Destination Server-192.168.233.214] in order to overwhelm and shut it down.

**3) Simulations After the Attack Had Happened**

Figure 23(a) and Figure 23(b) below show the effects of the attack launched

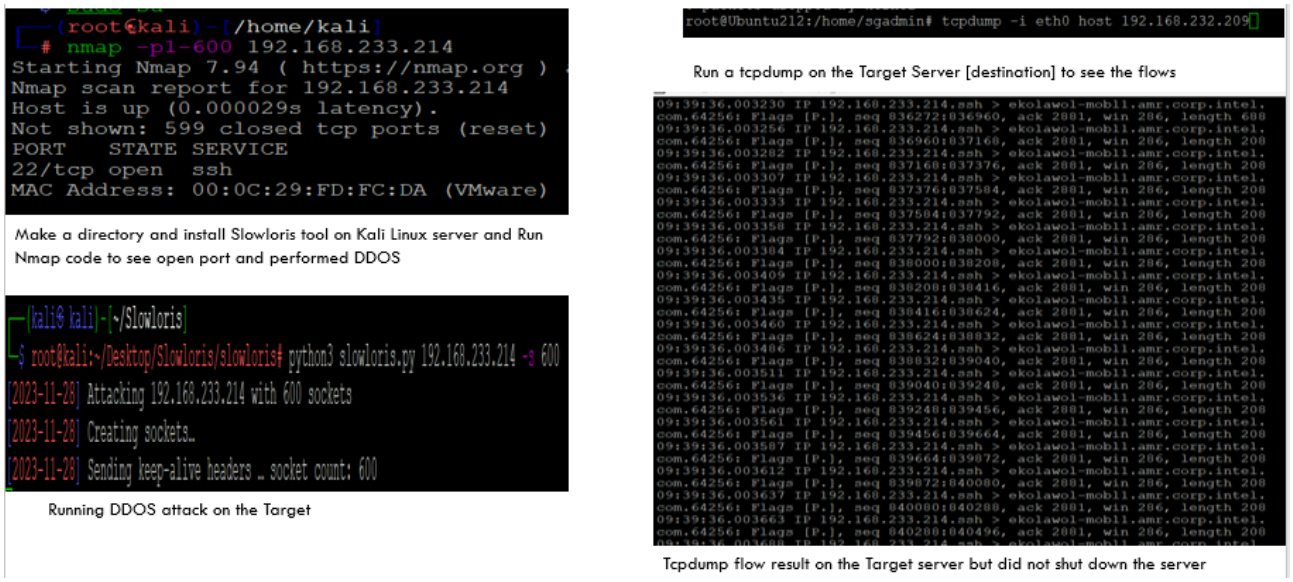
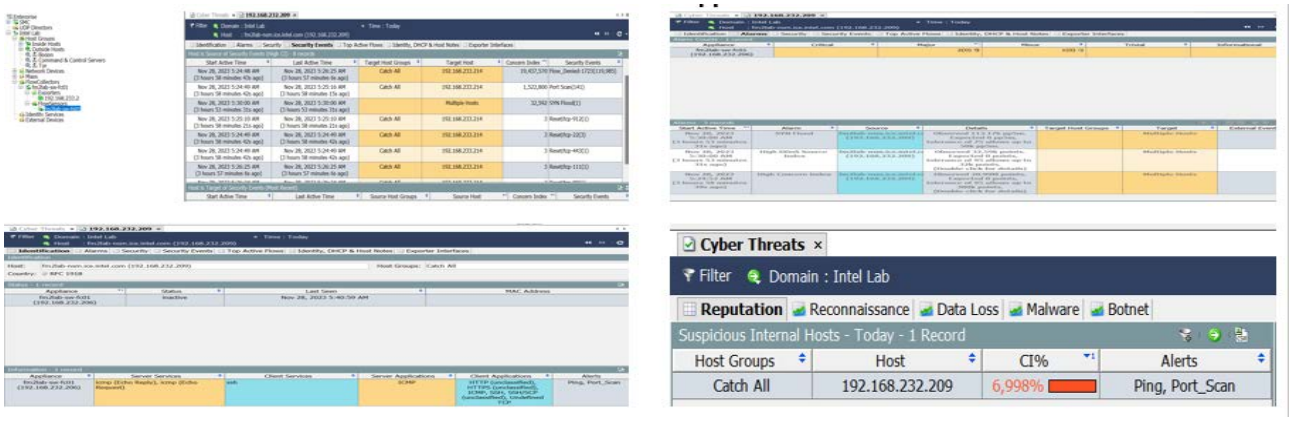
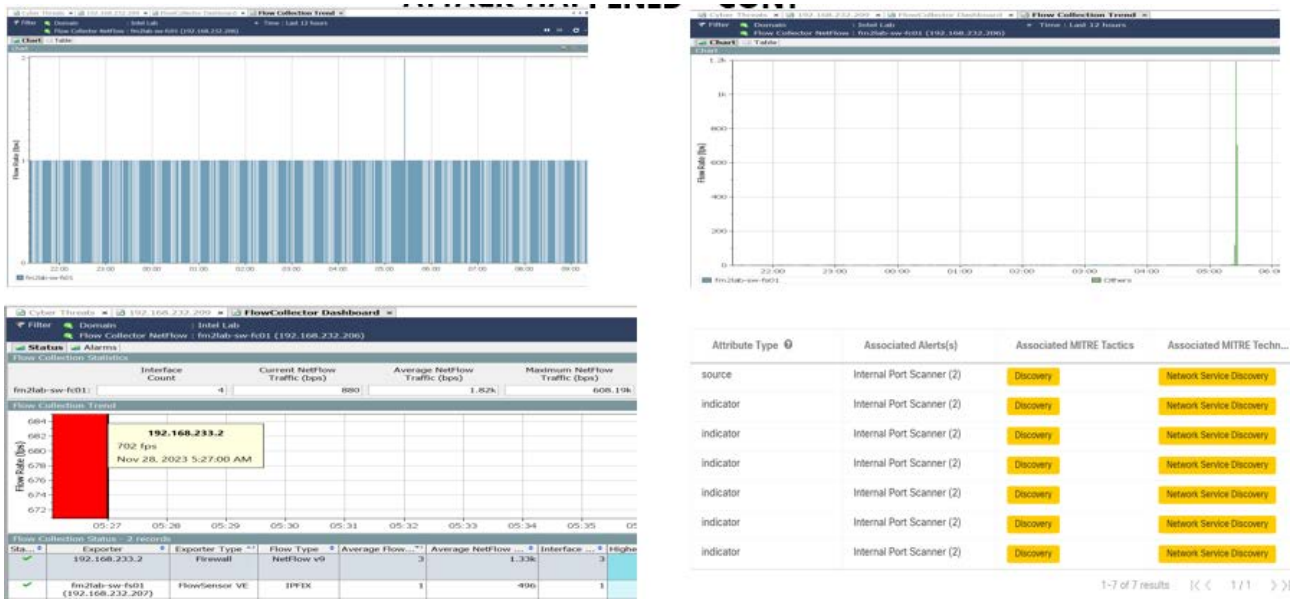


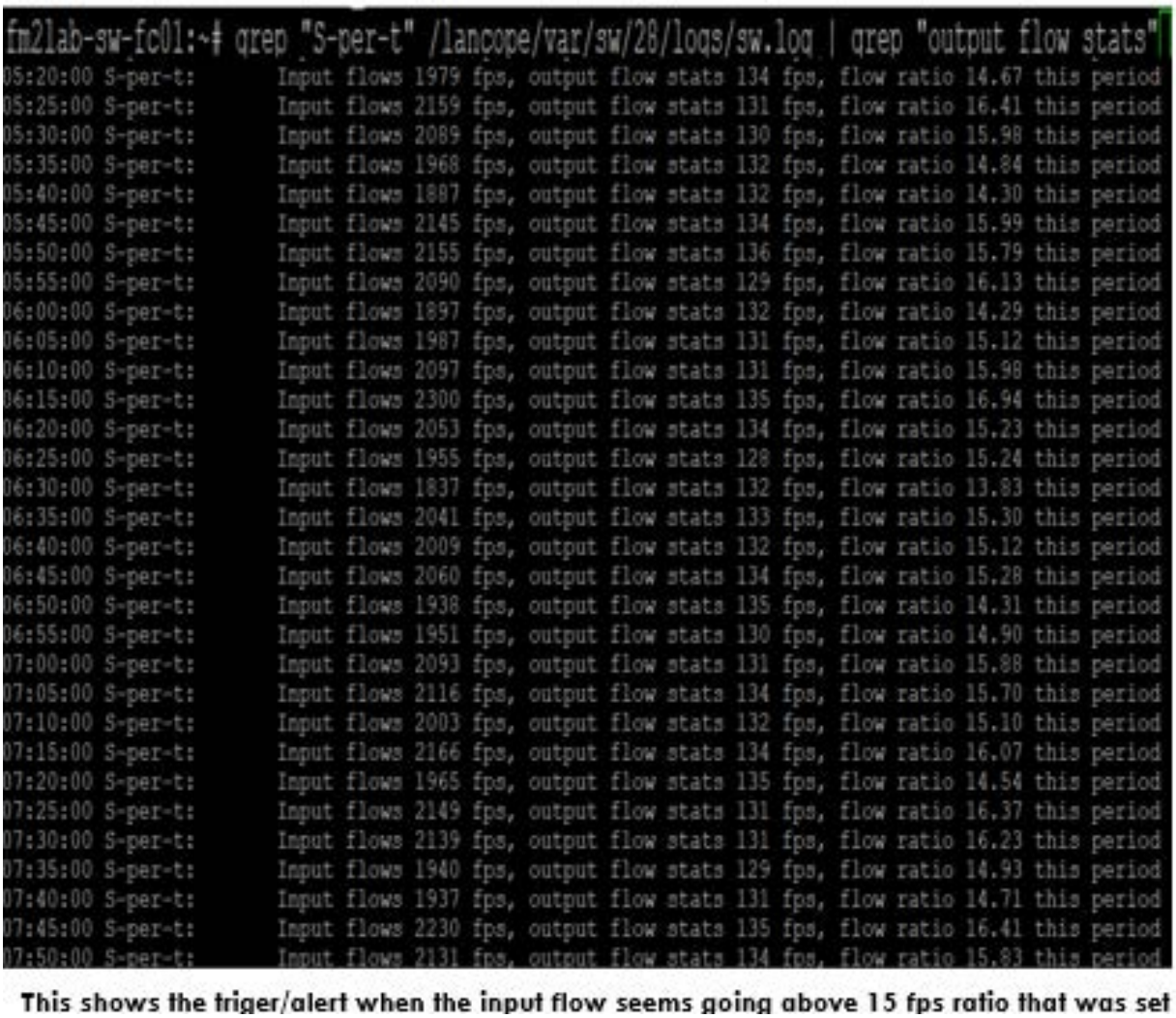

**Figure 22.** Stealthwatch simulations during and after the attack had happened.



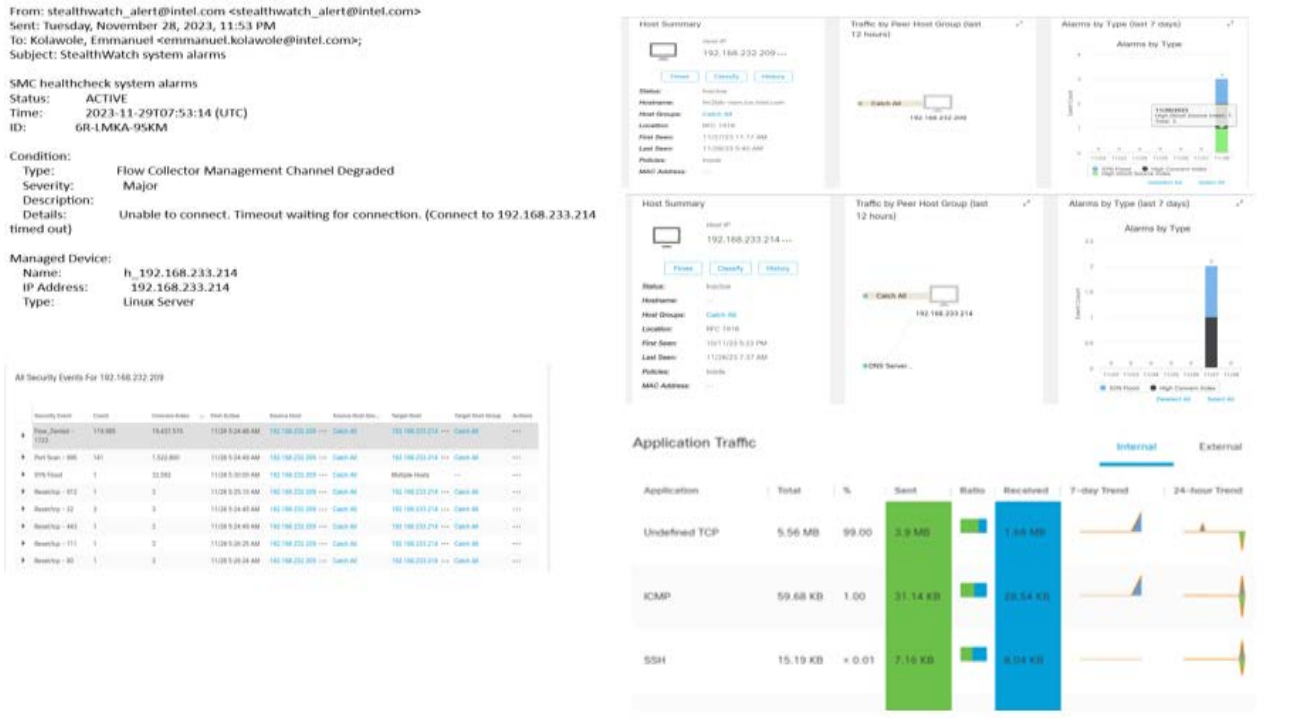

(a)


FlowCollector Dashboard
192.168.233.2
702 fps
Nov 28, 2023 5:27:00 AM
Attribute Type
Associated Alerts(s)
Associated MITRE Tactics
Associated MITRE Techn...
source
indicator
Internal Port Scanner (2)
Discovery
Network Service Discovery
1-7 of 7 results

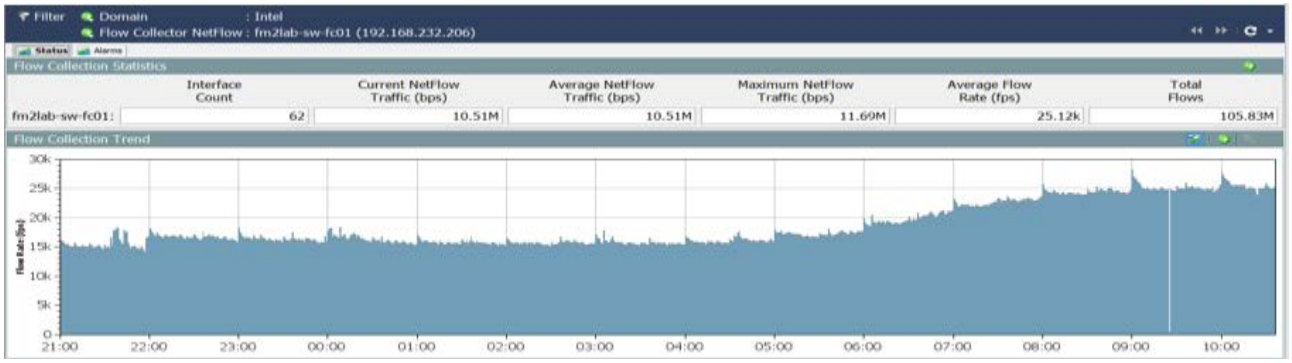
(b)


fm2lab-sw-fc01:~# grep "S-per-t" /lancope/var/sw/28/logs/sw.log | grep "output flow stats"
05:20:00 S-per-t: Input flows 1979 fps, output flow stats 134 fps, flow ratio 14.67 this period
05:25:00 S-per-t: Input flows 2159 fps, output flow stats 131 fps, flow ratio 16.41 this period
05:30:00 S-per-t: Input flows 2089 fps, output flow stats 130 fps, flow ratio 15.98 this period
05:35:00 S-per-t: Input flows 1968 fps, output flow stats 132 fps, flow ratio 14.84 this period
05:40:00 S-per-t: Input flows 1887 fps, output flow stats 132 fps, flow ratio 14.30 this period
05:45:00 S-per-t: Input flows 2145 fps, output flow stats 134 fps, flow ratio 15.99 this period
05:50:00 S-per-t: Input flows 2155 fps, output flow stats 136 fps, flow ratio 15.79 this period
05:55:00 S-per-t: Input flows 2090 fps, output flow stats 129 fps, flow ratio 16.13 this period
06:00:00 S-per-t: Input flows 1897 fps, output flow stats 132 fps, flow ratio 14.29 this period
06:05:00 S-per-t: Input flows 1987 fps, output flow stats 131 fps, flow ratio 15.12 this period
06:10:00 S-per-t: Input flows 2097 fps, output flow stats 131 fps, flow ratio 15.98 this period
06:15:00 S-per-t: Input flows 2300 fps, output flow stats 135 fps, flow ratio 16.94 this period
06:20:00 S-per-t: Input flows 2053 fps, output flow stats 134 fps, flow ratio 15.23 this period
06:25:00 S-per-t: Input flows 1955 fps, output flow stats 128 fps, flow ratio 15.24 this period
06:30:00 S-per-t: Input flows 1837 fps, output flow stats 132 fps, flow ratio 13.83 this period
06:35:00 S-per-t: Input flows 2041 fps, output flow stats 133 fps, flow ratio 15.30 this period
06:40:00 S-per-t: Input flows 2009 fps, output flow stats 132 fps, flow ratio 15.12 this period
06:45:00 S-per-t: Input flows 2060 fps, output flow stats 134 fps, flow ratio 15.28 this period
06:50:00 S-per-t: Input flows 1938 fps, output flow stats 135 fps, flow ratio 14.31 this period
06:55:00 S-per-t: Input flows 1951 fps, output flow stats 130 fps, flow ratio 14.90 this period
07:00:00 S-per-t: Input flows 2093 fps, output flow stats 131 fps, flow ratio 15.88 this period
07:05:00 S-per-t: Input flows 2116 fps, output flow stats 134 fps, flow ratio 15.70 this period
07:10:00 S-per-t: Input flows 2003 fps, output flow stats 132 fps, flow ratio 15.10 this period
07:15:00 S-per-t: Input flows 2166 fps, output flow stats 134 fps, flow ratio 16.07 this period
07:20:00 S-per-t: Input flows 1965 fps, output flow stats 135 fps, flow ratio 14.54 this period
07:25:00 S-per-t: Input flows 2149 fps, output flow stats 131 fps, flow ratio 16.37 this period
07:30:00 S-per-t: Input flows 2139 fps, output flow stats 131 fps, flow ratio 16.23 this period
07:35:00 S-per-t: Input flows 1940 fps, output flow stats 129 fps, flow ratio 14.93 this period
07:40:00 S-per-t: Input flows 1937 fps, output flow stats 131 fps, flow ratio 14.71 this period
07:45:00 S-per-t: Input flows 2230 fps, output flow stats 135 fps, flow ratio 16.41 this period
07:50:00 S-per-t: Input flows 2131 fps, output flow stats 134 fps, flow ratio 15.83 this period
This shows the triger/alert when the input flow seems going above 15 fps ratio that was set

(c)




(d)




(e)

**Figure 23.** (a) Stealthwatch simulations after the attack had happened; (b) Stealthwatch Simulations after the attack had happened—cont; (c) Flow collector input and output flow comparison; (d) Stealthwatch Simulations after the attack had happened—cont; (e) Stealthwatch simulations after the attack had happened—cont.

on the attack system or destination server by the attack client or source system. The Stealthwath tool was able to detect the attack based on the volume of traffics, ports in use and how consistently the attacker was trying to break into the destination server or target.

Figure 23(c) shows the input and output flow logs comparison of the DDoS effect and how the tool is able to mitigate the attack before it shuts down the destination server. As soon as the flow rate ratio seems above 15 fps (flow per second) a bit, the system generates alerts to notify the administrator of any suspected attack to take any proper action if any slips as shown in Figure 23(d). Thou, it has already mitigated the flow increase based on the baseline code/algorithm setup,

Firewall rules and IPS policy setup.

Figure 23(e) shows the simulation flow output on Stealthwatch tool after the attack which displayed little or no increase in flow level based on baseline set. Thou, there was a little increase in flow due to the excessive pings/Port scan, but the administrator was able to get the alert immediately based on the code/algorithm set to notify, if the flow goes above a 15 pfs. This then caused the administrator to investigate further without causing any shutting down of the server.

## 6. Conclusions

The Smart Grid has been developed due to the constantly growing distribution from renewable sources and with further aim to increase the efficiency, reliability, and safety of the existing power grid. This development has introduced new cyber-security challenges for the Smart Grid and is a very concerning issue because of emerging cyber-threats and security incidents that have occurred recently all over the world.

**1) The Pros and Cons**

In this research, we studied and found out the impact of DDoS attack in a WAMS communication network in Smart Grid by the co-simulation of GNS3, PMU connection tester. We then proposed the simulation of Optimized Stealthwatch Network Security System Tools to detect, mitigate and prevent DDoS attack in application to Smart Grid by also applying mechanism such as Firewall, Intrusion detection and Prevention Systems.

**2) Concluding Thoughts/Summary**

In this work, we proposed the system architecture of Stealthwatch Network Security System in Smart Grid. The impact of DDoS attack in a WAMS communication network has been studied and the efficient monitoring, detection and its mitigation was proposed through the optimization and modification of Stealthwatch simulation tool algorithms/codes. Also, we deployed Firewall & IPS systems to add to the detection and mitigation of DDoS attack in Smart Grid System. From the simulation results, we could see that the target system did not shut down nor degraded because of the source attack due to the mitigation strategies and alert system in place through Stealthwatch System Tools, IPS and Firewall in this research.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

[1] Wang, K., Du, M., Maharjan, S. and Sun, Y. (2017) Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. *IEEE Transactions on Smart Grid*, **8**, 2474-2482. https://doi.org/10.1109/tsg.2017.2670144

[2] Guo, Y., Ten, C., Hu, S. and Weaver, W.W. (2015) Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure. 2015 *IEEE Power & Energy*

*Society Innovative Smart Grid Technologies Conference*, Washington, 18-20 February 2015, 1-5. https://doi.org/10.1109/isgt.2015.7131828

[3] Asri, S. and Pranggono, B. (2015) Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. *Wireless Personal Communications*, **83**, 2211-2223. https://doi.org/10.1007/s11277-015-2510-3

[4] Eddy, J., Miner, N.E. and Stamp, J. (2017) Sandia's Microgrid Design Toolkit. *The Electricity Journal*, **30**, 62-67. https://doi.org/10.1016/j.tej.2017.04.002

[5] Sgouras, K.I., Birda, A.D. and Labridis, D.P. (2014) Cyber Attack Impact on Critical Smart Grid Infrastructures. *Innovative Smart Grid Technologies* 2014, Washington, 19-22 February 2014, 1-5. https://doi.org/10.1109/isgt.2014.6816504

[6] Yi, P., Zhu, T., Zhang, Q., Wu, Y. and Pan, L. (2016) Puppet Attack: A Denial of Service Attack in Advanced Metering Infrastructure Network. *Journal of Network and Computer Applications*, **59**, 325-332. https://doi.org/10.1016/j.jnca.2015.04.015

[7] Wei, J. and Kundur, D. (2012) A Flocking-Based Model for DoS-Resilient Communication Routing in Smart Grid. 2012 *IEEE Global Communications Conference*, Anaheim, 3-7 December 2012, 3519-3524. https://doi.org/10.1109/glocom.2012.6503660

[8] RF Wireless World (2012) Wireless Vendors and Resources. https://www.rfwireless-world.com/Articles/Smart-Grid-Architecture-basics-and-working.html

[9] Fang, B., Yin, X., Tan, Y., Li, C., Gao, Y., Cao, Y., *et al.* (2016) The Contributions of Cloud Technologies to Smart Grid. *Renewable and Sustainable Energy Reviews*, **59**, 1326-1331. https://doi.org/10.1016/j.rser.2016.01.032

[10] Otuoze, A.O., Mustafa, M.W. and Larik, R.M. (2018) Smart Grids Security Challenges: Classification by Sources of Threats. *Journal of Electrical Systems and Information Technology*, **5**, 468-483. https://doi.org/10.1016/j.jesit.2018.01.001

[11] Shrestha, M., Johansen, C., Noll, J. and Roverso, D. (2020) A Methodology for Security Classification Applied to Smart Grid Infrastructures. *International Journal of Critical Infrastructure Protection*, **28**, Article 100342. https://doi.org/10.1016/j.ijcip.2020.100342

[12] Demir, K., Ismail, H., Vateva-Gurova, T. and Suri, N. (2018) Securing the Cloud-Assisted Smart Grid. *International Journal of Critical Infrastructure Protection*, **23**, 100-111. https://doi.org/10.1016/j.ijcip.2018.08.004

[13] Ylmaz, E.N., Ciylan, B., Gonen, S., Sindiren, E. and Karacayilmaz, G. (2018) Cyber Security in Industrial Control Systems: Analysis of DoS Attacks against PLCs and the Insider Effect. 2018 6*th International Istanbul Smart Grids and Cities Congress and Fair*, Istanbul, 25-26 April 2018, 81-85. https://doi.org/10.1109/sgcf.2018.8408947

[14] Liu, R., Vellaithurai, C., Biswas, S.S., Gamage, T.T. and Srivastava, A.K. (2015) Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Transactions on Smart Grid*, **6**, 2444-2453. https://doi.org/10.1109/tsg.2015.2432013

[15] Efthymiou, C. and Kalogridis, G. (2010) Smart Grid Privacy via Anonymization of Smart Metering Data. 2010 *First IEEE International Conference on Smart Grid Communications*, Gaithersburg, 4-6 October 2010, 238-243. https://doi.org/10.1109/smartgrid.2010.5622050

[16] Pour, M.M., Anzalchi, A. and Sarwat, A. (2017) A Review on Cyber Security Issues and Mitigation Methods in Smart Grid Systems. *SoutheastCon* 2017, Concord, 30 March-2 April 2017, 1-4. https://doi.org/10.1109/secon.2017.7925278

[17] Yadav, T. and Rao, A.M. (2015) Technical Aspects of Cyber Kill Chain. In: Abawajy,

J.H., Mukherjea, S., Thampi, S.M. and Ruiz-Martínez, A., Eds., *Security in Computing and Communications*, Springer International Publishing, 438-452. https://doi.org/10.1007/978-3-319-22915-7_40

[18] Cisco (n.d.) Cisco Models Specifications. https://cisco.com