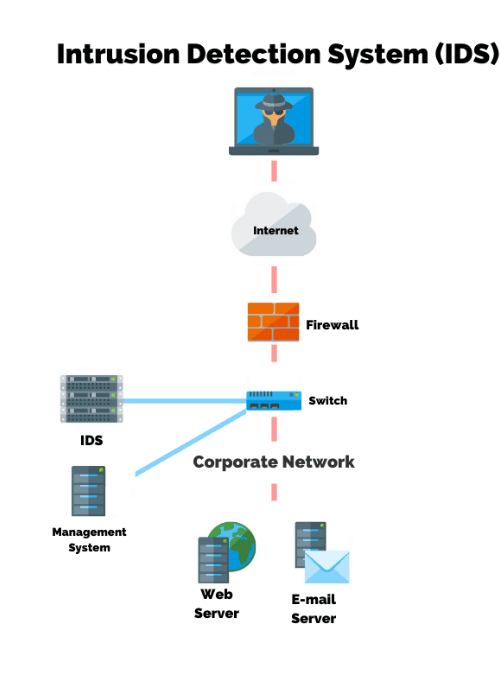
**COMPUTER NETWORKS**

**Case Study**

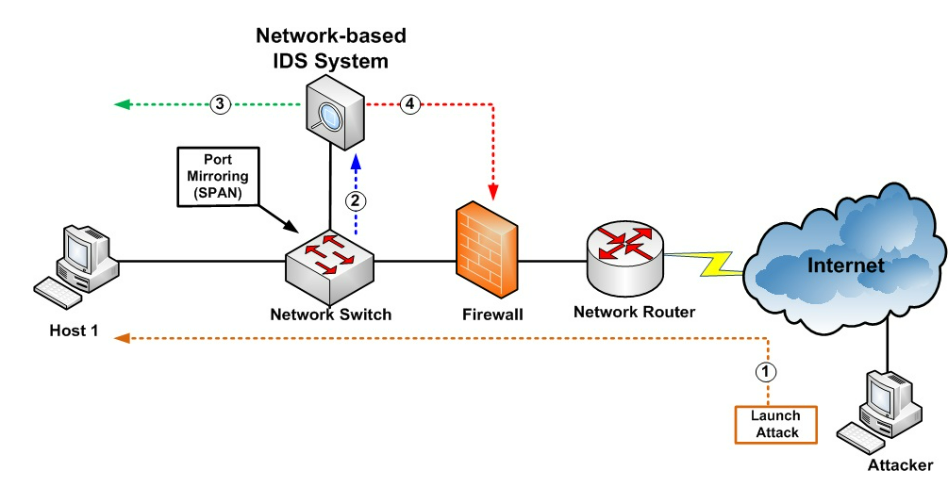
**TOPIC NAME – INTRUSION DETECTION SYSTEM**



|  |  |  |
| --- | --- | --- |
| **ROLL NUMBER** | **NAME** |  |
| **CB.EN.U4CSE21042** | **Sheshu P** |  |
| **CB.EN.U4CSE21047** | **Reshiha RG** |  |
| **CB.EN.U4CSE21063** | **T Vinay Kumar** |  |

**PROBLEM STATEMENT:**

The evolution of malicious software (malware) poses a critical challenge to the design of intrusion detection systems (IDS). Malicious attacks have become more sophisticated and the foremost challenge is to identify unknown and obfuscated malware, as the malware authors use different evasion techniques for information concealing to prevent detection by an IDS. In addition, there has been an increase in security threats designed to target internet users. Therefore, computer security has become essential as the use of information technology has become part of our daily lives.



**WHAT IS AN IDS IN NETWORKS?**

* Intrusion detection systems, or more specifically network intrusion detection systems, provide a solution that examines incoming and outgoing network traffic from servers and clients to detect any type of malicious activity.
* Intrusion detection systems (IDSs) are an important part of the defence mechanisms through which continuous monitoring of the system is performed.
* An IDS is a software or hardware system that identifies malicious actions on computer systems in order to allow for system security to be maintained. The goal of an IDS is to identify different kinds of malicious network traffic and computer usage, which cannot be identified by a traditional firewall. This is vital to achieving high protection against actions that compromise the availability, integrity, or confidentiality of computer systems.

**TYPES OF IDS:**

**Network-Based:**

A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity.

**Wireless:**

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyze network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs.

**Network Behaviour Anomaly Detection:**

Network behaviour anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs.

**Host-Based:**

Host-based intrusion detection systems (HIDS) analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more.

**Detection Types**

1. **Signature-Based Detection**

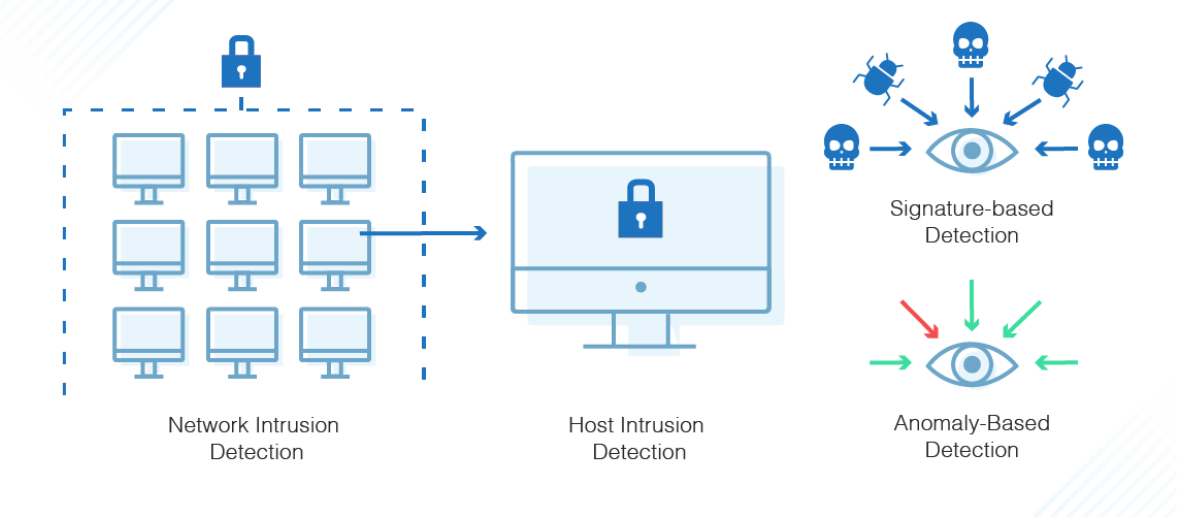
An IDS can use signature-based detection, relying on known traffic data to analyse potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a Signature based IDS.

1. **Anomaly-Based Detection**

An IDS that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly-based detection. This method is useful for detecting unwanted traffic that is not specifically known. For instance, an anomaly-based IDS will detect that an Internet protocol (IP) packet is malformed.

1. **Stateful Protocol Inspection**

Stateful protocol inspection is similar to Anomaly based detection, but it can also analyse traffic at the network and transport layer and vender-specific traffic at the application layer, which anomaly-based detection cannot do.



**LITERATURE REVIEW:**

**Introduction:**

* In recent years, the escalating frequency and sophistication of cyber-attacks have underscored the critical need for robust security measures. Intrusion Detection Systems (IDS) have emerged as a pivotal component in safeguarding computer networks and systems from unauthorized access, malicious activities, and potential threats. This literature review aims to provide a comprehensive overview of the key developments, challenges, and advancements in the field of Intrusion Detection Systems.
* The origins of Intrusion Detection Systems can be traced back to early research in the 1970s. The initial focus was on anomaly detection, where deviations from normal network behavior were flagged as potential threats. Over the years, the field has evolved to include signature-based detection, which involves matching predefined patterns of known attacks. The integration of machine learning techniques, artificial intelligence, and big data analytics has further propelled the capabilities of IDS.

**Challenges in Intrusion Detection:**

Despite the progress made in IDS, several challenges persist. These challenges encompass issues like false positives and false negatives, the need for real-time detection, scalability concerns, and the ability to handle encrypted traffic. Researchers continue to address these challenges to ensure the efficacy and reliability of IDS in diverse and dynamic environments.

**Future Directions and Emerging Trends:**

The literature review concludes by exploring potential future directions in the field of Intrusion Detection Systems. As cyber threats evolve, there is a growing emphasis on the development of adaptive and self-learning IDS that can autonomously adjust to new attack vectors. Additionally, the integration of threat intelligence feeds, collaborative detection, and the use of Explainable AI (XAI) techniques are identified as emerging trends in the continuous evolution of IDS.

**MOTIVATION:**

The primary motivation behind Intrusion Detection Systems (IDS) in networks, both in theory and practice, is to enhance the overall cybersecurity posture by identifying and responding to potential security incidents. Here are several key motivations behind the deployment of IDS in both network environments and the real world:

1. **Early Detection of Intrusions:**

**Prevention is not foolproof:** While firewalls and other security measures are designed to prevent unauthorized access, they may not catch every potential threat. IDS acts as a complementary layer by detecting and alerting on suspicious activities that might indicate a security breach.

1. **Identification of Anomalies:**

**Unusual Patterns and Behaviors:** IDS is designed to detect anomalies and patterns that deviate from normal network behavior. This can include unusual traffic patterns, unexpected access attempts, or abnormal system activities.

1. **Timely Incident Response:**

**Minimizing Downtime:** Rapid detection allows for quicker incident response, reducing the potential impact of a security breach. Identifying and mitigating threats promptly can prevent further damage and minimize downtime.

1. **Monitoring and Visibility:**

**Comprehensive Network Visibility:** IDS provides administrators with a comprehensive view of network traffic and system activities. This visibility is crucial for understanding the security landscape and making informed decisions about network security policies.

1. **Compliance Requirements:**

**Regulatory Compliance:** Many industries and organizations are subject to regulatory requirements that mandate the implementation of security measures, including intrusion detection. IDS helps organizations comply with standards such as HIPAA, PCI DSS, and others.

1. **Protection Against Evolving Threats:**

**Adaptability to New Threats:** Cyber threats are constantly evolving. IDS, particularly those utilizing advanced technologies like machine learning, can adapt to new and emerging threats that might not be recognized by traditional security mechanisms.

1. **Insider Threat Detection:**

**Identifying Insider Misuse:** IDS can help identify insider threats or misuse of authorized access. This is crucial for detecting activities that may be malicious or indicate compromised credentials.

1. **Forensic Analysis:**

**Post-Incident Analysis:** IDS logs and alerts contribute to forensic analysis after a security incident. Understanding the nature and scope of an intrusion is essential for improving security measures and preventing future incidents.

1. **Risk Management:**

**Risk Mitigation:** By providing continuous monitoring and threat detection, IDS contributes to proactive risk management. Identifying vulnerabilities and addressing them helps organizations reduce the overall risk of cyber threats.

1. **Security Awareness:**

**Educating Security Personnel:** IDS alerts serve as educational tools for security personnel, enabling them to understand and respond to various types of cyber threats. This ongoing learning process enhances the overall cybersecurity awareness within an organization.

The real-world motivation behind Intrusion Detection Systems is multifaceted, encompassing the need for early threat detection, incident response, compliance, risk management, and overall improvement of network security. As cyber threats continue to evolve, the role of IDS remains critical in maintaining a resilient and secure network environment.

**Software Tools:**

**GNS3 integrated with VMWare For IDS:**

* Use GNS3 to design a network topology that represents the environment where you want to deploy the IDS. This may include routers, switches, firewalls, and various network segments.
* Emulate the network devices that will be present in the environment. For IDS testing, these devices may include routers, switches, and servers.
* Deploy the IDS within the simulated network. This could be a dedicated IDS appliance or software-based IDS, depending on your preference and the specific IDS solution you want to test.
* Simulate network taps or SPAN ports to mirror traffic to the IDS. This involves connecting the IDS to the appropriate network segments or devices to ensure it can analyze all relevant traffic.
* Generate realistic network traffic within the GNS3 environment to simulate real-world scenarios. This traffic should include normal network activities and potential malicious activities that the IDS needs to detect.
* Configure the IDS rules based on the types of attacks or anomalies you want to test. The rules define the criteria that the IDS will use to identify potential threats.
* Run simulations in GNS3 to generate traffic and test the effectiveness of the IDS. Analyze the IDS alerts and logs to assess its ability to detect and respond to different types of security events.
* Based on the results of your testing, fine-tune the IDS configurations and rules to optimize its performance. This iterative process helps enhance the accuracy and efficiency of the IDS in identifying threats.
* Integrate logging and monitoring tools within GNS3 to capture and analyze logs generated by the IDS. This provides a more comprehensive view of security events within the simulated network.
* If applicable, simulate scenarios where the network scales or experiences increased traffic loads. Evaluate the IDS's performance under varying conditions to ensure it can handle the demands of a dynamic network.

**HOW IS SNORT USED FOR IDS:**

Snort is a versatile Intrusion Detection System (IDS) that uses a combination of protocols and rules to monitor and detect various types of attacks. When using Snort within a GNS3 environment, you can configure it to analyze network traffic and generate alerts based on predefined rules.

**Rules:**

Snort uses a rule-based detection engine where rules are defined to identify specific patterns or behaviors indicative of attacks. Each rule is written in a specific format and consists of various components, including:

**Rule Header:**

Specifies the action to take (alert, log, etc.).

Defines the protocol to inspect (TCP, UDP, ICMP, IP, etc.).

Specifies source and destination IP addresses, ports, and other criteria.

**Rule Options:**

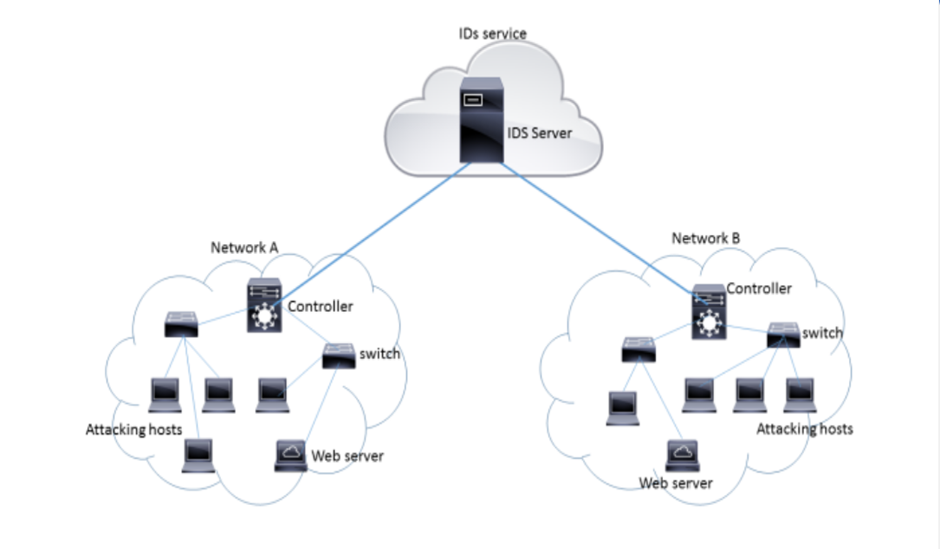
Contains content matches, which are patterns or signatures indicative of attacks.

May include additional metadata, such as the message to log on detection.

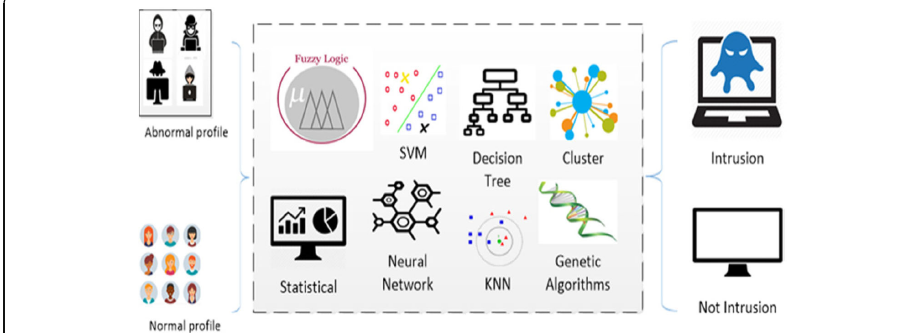
**EXAMPLE:**

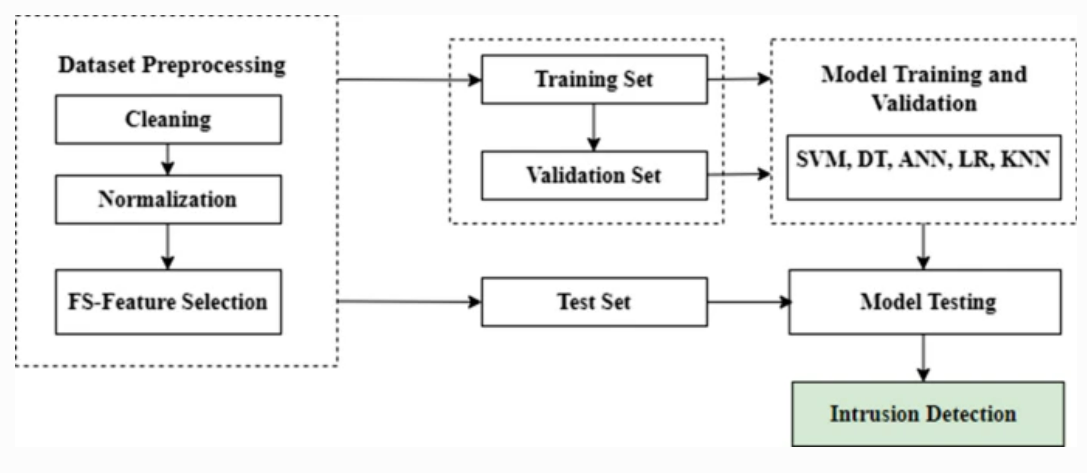
1. Intrusion Detection System (IDS) rules in Snort are typically defined to detect various network activities, and they can include rules for monitoring ICMP (Internet Control Message Protocol) traffic, commonly associated with the ping utility. The following is an example of a simple Snort rule designed to detect ICMP echo request (ping) packets:

alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"PING detected"; sid:1000001;)



**ML Based IDS Architecture**:





**Attacks Demonstrated:**

**1. ICMP**

**2. MAC Flooding**

**3. DOS SYN attack**

**4. UDP Flooding**

**Tools and Environments used :**

**GNS3:**

GNS3 (Graphical Network Simulator-3) is an open-source network emulation software used for designing, simulating, and testing complex network topologies.

Supported Devices:

GNS3 supports a variety of virtualized network devices, including routers (Cisco, Juniper, etc.), switches (Cisco IOS switches), and virtual PCs.

**Security Onion:**

**Introduction:**

Purpose: Security Onion is an open-source platform designed for network security monitoring (NSM) and intrusion detection (IDS).

Components: It integrates various security tools to provide a comprehensive solution for monitoring, analyzing, and responding to security events.

**Key Components:**

Snort and Suricata: Powerful open-source IDS engines for detecting and alerting on network traffic anomalies.

**Deployment**:

Live Monitoring: Can be deployed for real-time monitoring of network traffic.

Packet Capture: Collects and analyzes network packets for detailed insights.

**Use Cases:**

Incident Detection: Security Onion aids in the detection of security incidents and potential threats on the network.

Threat Hunting: Provides tools for proactively searching for and analyzing security threats within the network.

Forensic Analysis: Supports forensic investigations by capturing and storing network activity for analysis.

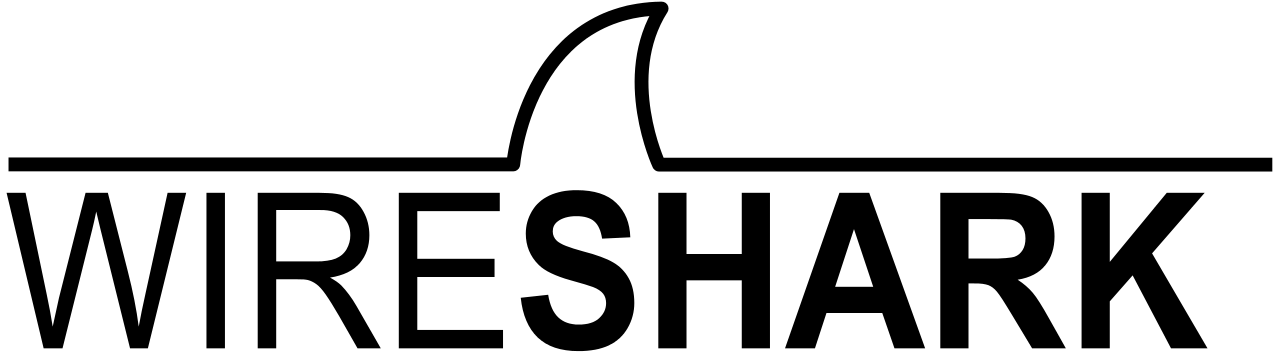
Scalability:

**Wireshark :**

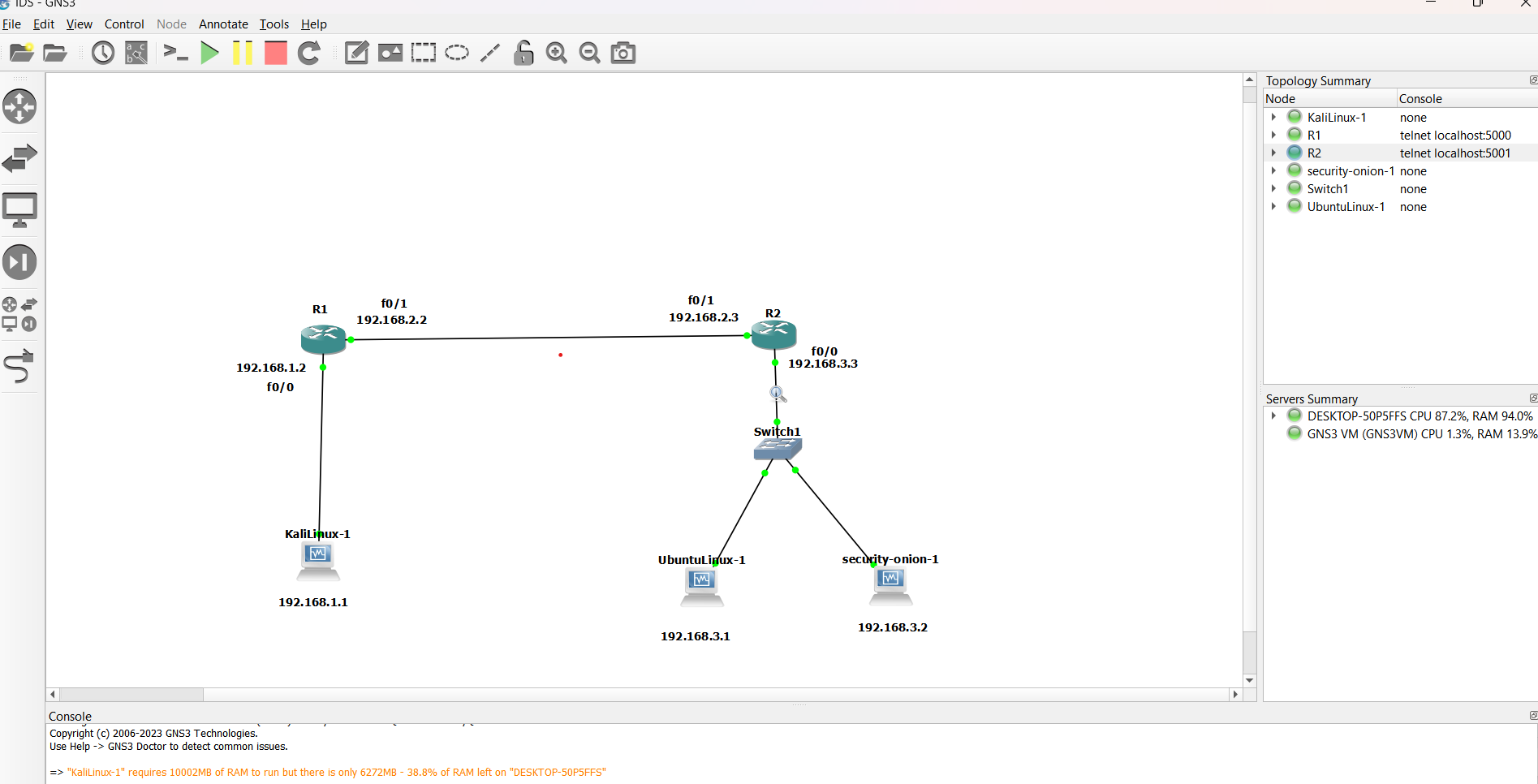
Wireshark is a widely-used open-source network protocol analyzer that allows users to capture and inspect network traffic in real-time. With a user-friendly interface, Wireshark provides detailed packet-level analysis, helping troubleshoot network issues and identify security threats. It supports a wide range of protocols, making it a versatile tool for network professionals. Wireshark offers powerful filtering and search capabilities, enabling users to focus on specific network packets. Its active community and regular updates contribute to its status as an essential tool for network monitoring and analysis.







**Topology used for Attack Demonstration:**

****

**Layers Involved:**

MAC flooding primarily occurs at the Data Link Layer (Layer 2) of the OSI (Open Systems Interconnection) model.

TCP SYN flooding occurs at the Transport Layer (Layer 4) of the OSI (Open Systems Interconnection) model

A UDP (User Datagram Protocol) flooding attack occurs at the Transport Layer (Layer 4) of the OSI (Open Systems Interconnection) model

ICMP (Internet Control Message Protocol) flooding attack occurs at the Network Layer (Layer 3) of the OSI (Open Systems Interconnection) model.

**ICMP Flooding:**

**ICMP Overview:**

ICMP is a network layer protocol used to send error messages and operational information about network conditions.

Commonly associated with the "ping" command, ICMP is essential for network troubleshooting.

ICMP Flooding Attack Basics:

ICMP flooding involves sending a massive number of ICMP packets to a target system in a short period.

The goal is to overwhelm the target's network infrastructure, consuming its resources and making it unresponsive.

**Attack Techniques:**

**Ping Flood:**

Also known as a "ping of death," attackers use the ping command to send a large number of ICMP echo request packets to the target.

The target system becomes inundated with ICMP requests, leading to performance degradation.

**Impact of ICMP Flooding:**

**Denial of Service (DoS):**

Overloading the target system's resources leads to a denial of service, making it unresponsive to legitimate users.

Network Congestion:

The sheer volume of ICMP packets can congest the target's network, affecting normal network operations.

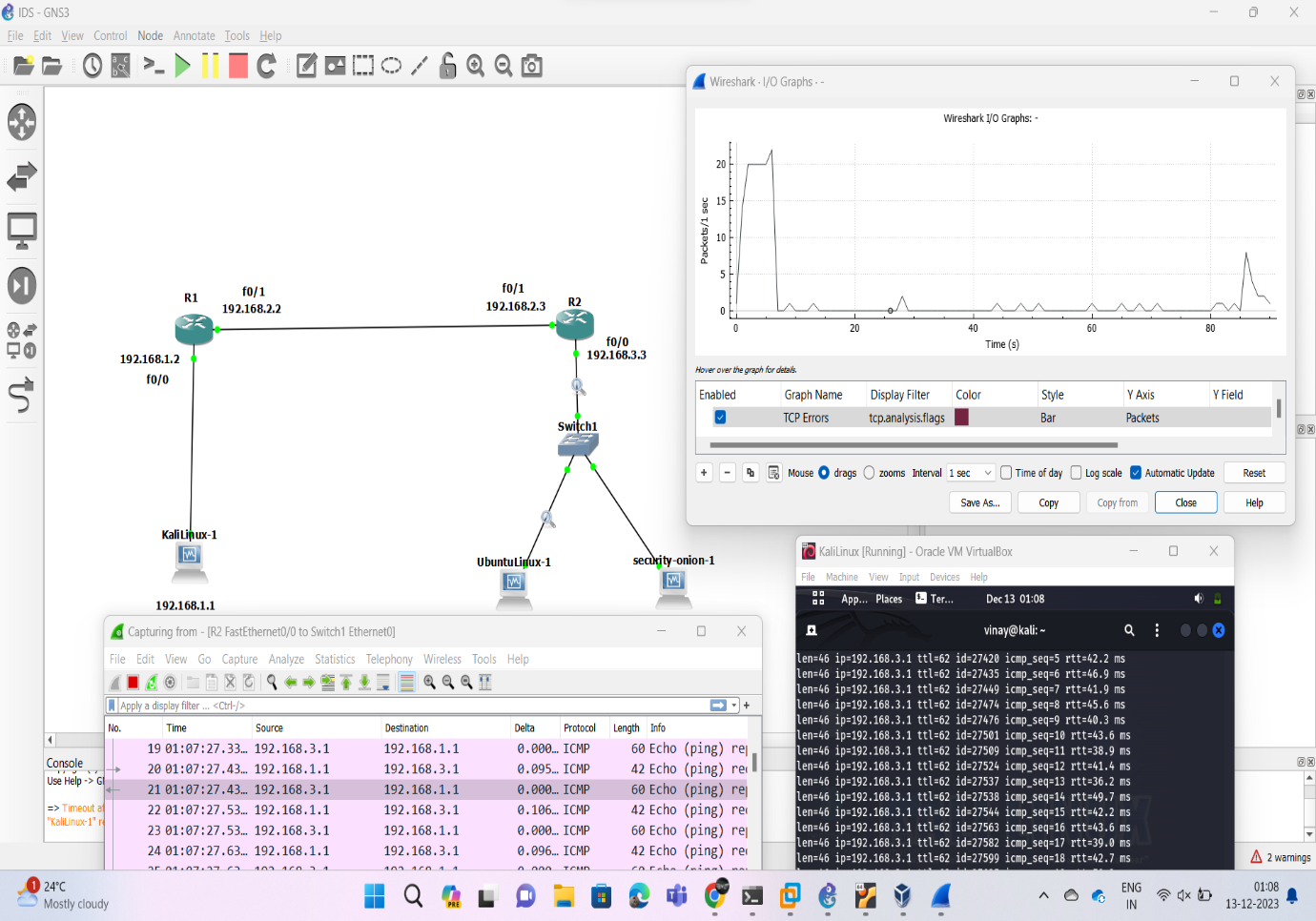
**Detection and Mitigation**:

**Intrusion Detection Systems (IDS):**

IDS can be employed to detect patterns indicative of ICMP flooding.

Firewalls and Rate Limiting:

Firewalls can be configured to block or limit the rate of incoming ICMP traffic.



**MAC Flooding:**

**Objective:**

MAC (Media Access Control) flooding is a network attack that aims to overwhelm the MAC address table of a switch.

**Attack Mechanism:**

Flood the switch with a large number of fake MAC addresses, exhausting the available space in the MAC address table.

**Impact:**

Once the MAC address table is full, the switch enters into a fail-open state, treating all incoming traffic as broadcast, leading to network congestion and potential denial of service.

**Attackers' Advantage:**

Attackers can use MAC flooding to conduct other attacks like sniffing unicast traffic or launching Man-in-the-Middle attacks by intercepting and forwarding network traffic.

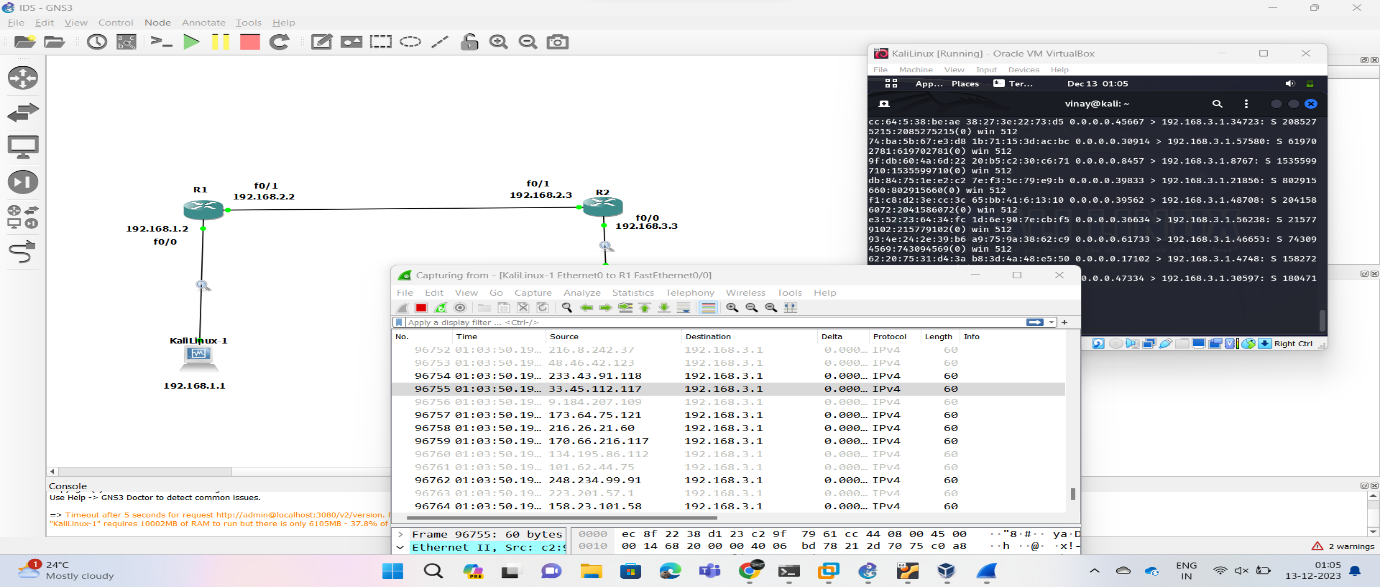
**Detection and Mitigation**:

Use tools like MAC limiting and sticky MAC addresses to enhance security against MAC flooding attacks.

Employ network monitoring and intrusion detection systems to detect unusual patterns of MAC address activity.

Regularly update switch firmware and apply security best practices to mitigate vulnerabilities.

IDS can be employed to detect patterns indicative of MAC.



**SYN DOS:**

**Objective**:

TCP SYN (Synchronization) Denial-of-Service (DoS) attack aims to overwhelm a target system by flooding it with a high volume of TCP SYN requests.

**Attack Method:**

Attackers send a large number of SYN requests to the target, initiating the TCP handshake process without completing it.

Resource Exhaustion:

The target system allocates resources for each incoming SYN request, creating half-open connections that consume memory and other system resources.

Denial of Service:

As the number of half-open connections increases, the target becomes unable to handle legitimate connection requests, leading to service degradation or unavailability.

**TCP Handshake Disruption:**

The attack disrupts the normal TCP three-way handshake process, preventing the establishment of complete connections and resulting in network congestion.

**Amplification and Reflection:**

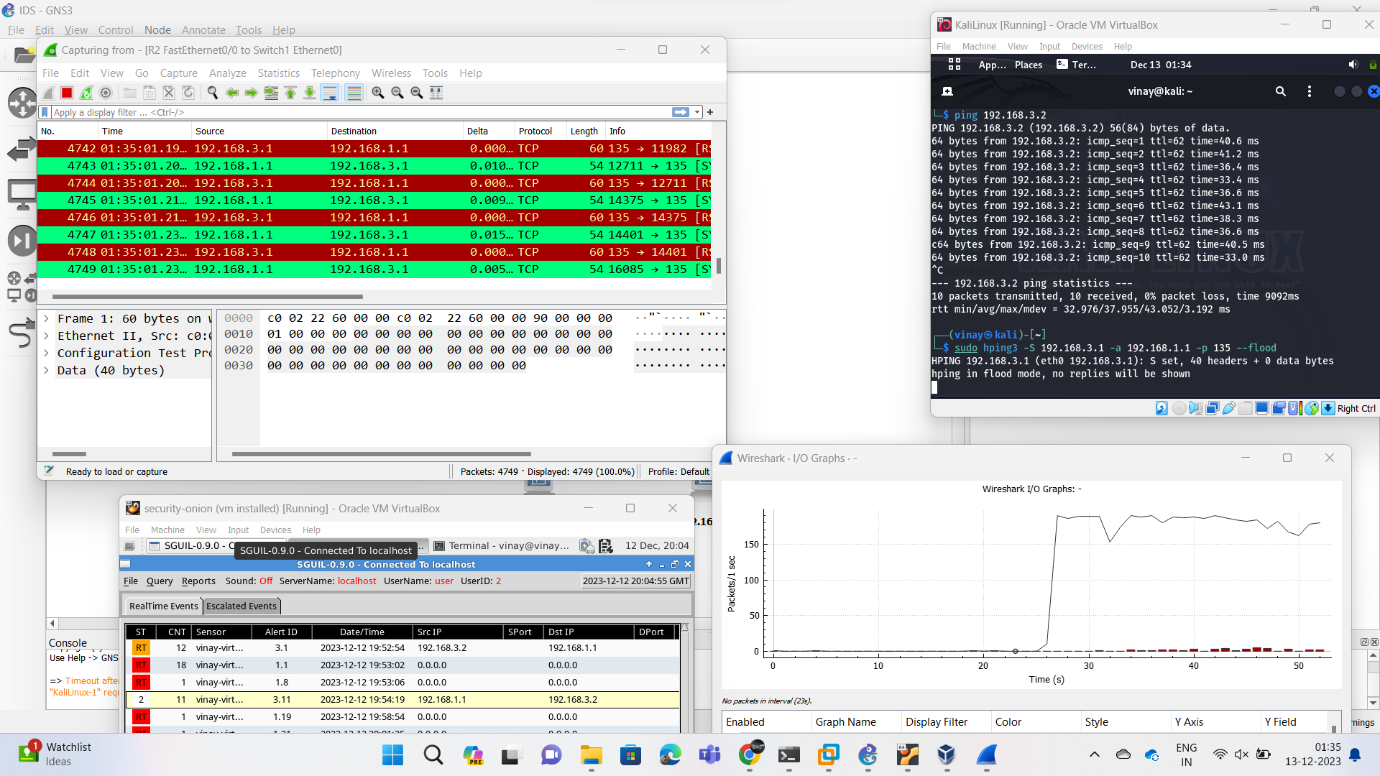
Attackers may use amplification techniques or reflection from other systems to increase the volume of SYN requests, intensifying the impact of the attack.

**Mitigation Strategies:**

Implementing SYN cookies, a technique to mitigate SYN flooding by not allocating resources until the three-way handshake is completed.

Employing rate limiting and connection threshold policies on network devices to filter out excessive SYN requests.

Utilizing intrusion prevention systems (IPS) and firewalls to detect and block malicious SYN traffic.



**UDP Amplification attack :**

**Objective:**

UDP (User Datagram Protocol) amplification attacks aim to overwhelm a target system or network by exploiting UDP-based services to generate and amplify traffic.

**Attack Method:**

Attackers send small UDP packets with a forged source address to open UDP services, causing responses to be sent to the victim, amplifying the volume of data directed at the target.

Amplification Factor:

The attack leverages services that generate larger responses than the size of the initial request, leading to an amplification of the attack traffic.

Reflection:

Attackers often use reflection techniques, bouncing the attack traffic off multiple servers or devices, making it difficult to trace the origin of the attack.

**Targeted Services:**

Commonly exploited UDP services include DNS (Domain Name System), NTP (Network Time Protocol), SNMP (Simple Network Management Protocol), and others that respond to requests with larger payloads.

Impact:

UDP amplification attacks can lead to network congestion, service disruption, and, in severe cases, denial of service for the targeted system.

**DNS Amplification:**

A specific type of UDP amplification where attackers send DNS queries with a spoofed source IP, causing DNS servers to respond to the victim with larger DNS responses.

**Mitigation Strategies:**

Filtering and rate-limiting UDP traffic on network devices to mitigate the impact of amplification attacks.

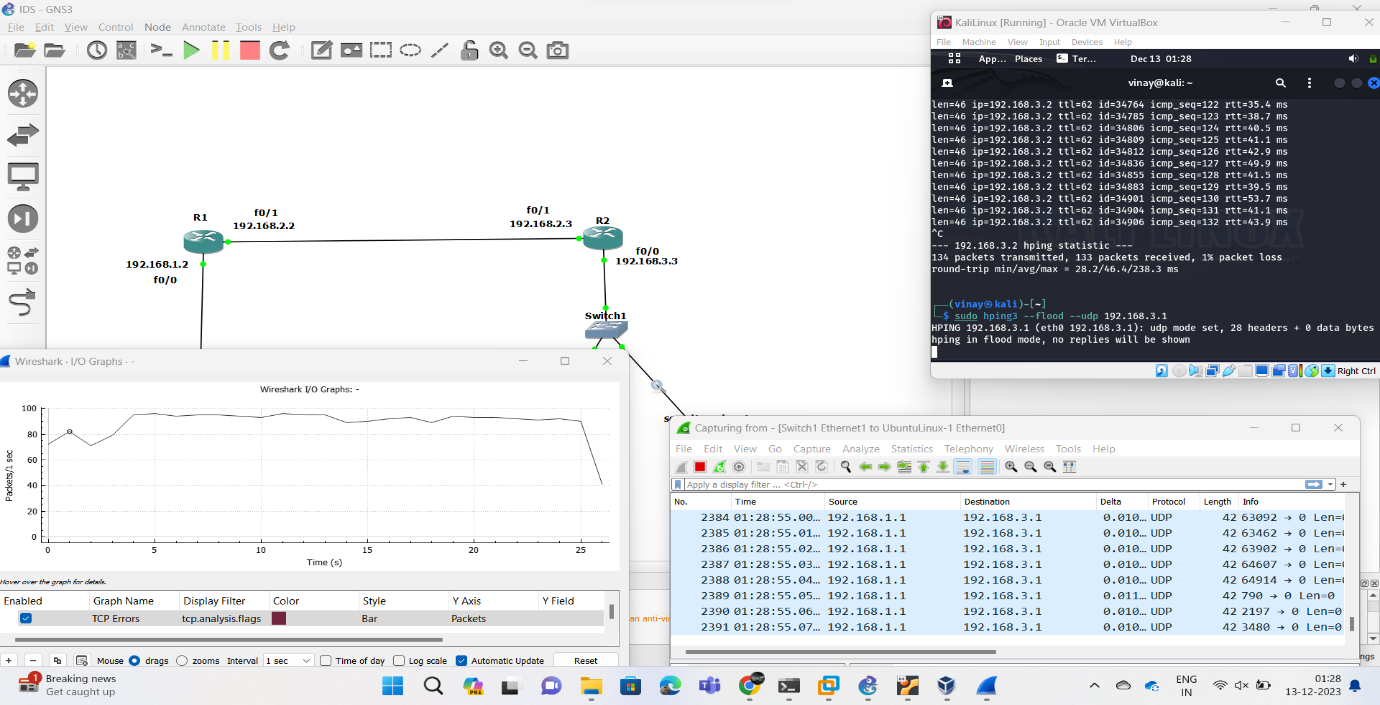
Configuring firewall rules to block or limit traffic from known malicious sources.

Implementing source address validation to reduce the effectiveness of IP address spoofing.

**Monitoring and Detection:**

Utilizing intrusion detection and prevention systems to detect patterns indicative of UDP amplification attacks.

Monitoring network traffic for sudden increases in UDP traffic, especially to vulnerable services.



**Research Papers as References:**

**GNS3 Approach:**

**PAPER:** [**https://ieeexplore.ieee.org/document/9030472**](https://ieeexplore.ieee.org/document/9030472)

The simulation model of the corporate

network protection system based on GNS3 is constructed.

The GNS3 program is a graphical network emulator that

allows to simulate a virtual network of more than 20

different manufacturers on a local computer, attach a virtual

network to the real network. Corporate network information

protection system includes Gateway, Firewall, Digital

Signature Verifier and Logger services. SQL Injection and

Cross-site Scripting threat protection are implemented.

Digital Signature Verification provides an additional layer of

information security. The stress testing conducted by the

Vega (Kali Linux) program showed that the system is

extremely resistant to SQL Injection and Cross-site scripting

attacks. The simulation model of the corporate network

protection system based on GNS3 is developed using the

minimum size of the digital signature to ensure a given level

of stability.

**PAPER:** [**https://www.researchgate.net/publication/308704382\_Development\_of\_a\_virtualized\_networking\_lab\_using\_GNS3\_and\_VMware\_workstation**](https://www.researchgate.net/publication/308704382_Development_of_a_virtualized_networking_lab_using_GNS3_and_VMware_workstation)

The goal of this project is to create a powerful alternative

tool to physical networking equipment available at CSU

Sydney. GNS3 can be used to make a virtual network with full

network device operating systems (IOS). The end devices can

be connected to Virtual machines running full operating

systems using VMware Workstation. One of the major

advantages of having a lab in a virtual environment is that the

resources can be easily replicated. For example, a single

virtual image of a router or a desktop computer can easily be

replicated and deployed across the network. Similarly,

multiple network adapters can be created from one physical

network card through virtualization using VMware

Workstation. However, the number of virtual instances

that can be created will be limited by the hardware capacity of

the physical host computer.

The model we will be using for the lab will have GNS3 as the

main tool deploying the simulated network. VMware, on the

other hand, will be used to create virtual network adapters and

assign them to the Virtual Machines with full Operating

Systems running on them. A model explaining

how the lab is deployed using a basic triangular 3-router

configuration.

**PAPER:**

[**https://www.researchgate.net/publication/347912059\_Analysis\_of\_Different\_Types\_of\_Network\_Attacks\_on\_the\_GNS3\_Platform**](https://www.researchgate.net/publication/347912059_Analysis_of_Different_Types_of_Network_Attacks_on_the_GNS3_Platform)

In this study, DDoS, SQL injection and XSS attacks that hackers use most in cyber attacks are modeled on GNS3 emulator platform and network security is analyzed. A network scenario was designed using Graphical Network Simulator (GNS3), virtual machines, VMware workstation, firewall, router, and switches in order to examine the attacks on networks in real environment. Attacks were performed on this network with different techniques and target servers and devices were affected by the attacks. At the time of the attack, network traffic between the attacker and the target device was recorded with Wireshark software. Network traffic records and traces were examined and evaluations of attacks were made.

**PAPER:**

[**https://ieeexplore.ieee.org/document/10336165**](https://ieeexplore.ieee.org/document/10336165)

Multicast networks, while efficient in data

transmission, are susceptible to targeted attacks. Leveraging

GNS3's capabilities, this study emulates and analyzes three

types of multicast attacks: fake rendezvous point attack, IGMP

flood, and IGMP Leave attacks. Through realistic emulation

performed via GNS3, the research sheds light on attack

implementation. The results offer insights into investigating

multicast vulnerabilities, benefiting security practitioners and

researchers alike. This work enhances understanding of

multicast network attacks, presenting a practical approach to

evaluating and investigating against potential threats.

The study highlights the vulnerability of multicast networks to targeted attacks despite their efficiency in data transmission. Through the effective utilization of GNS3’s capabilities, this study successfully emulated and analyzed three specific types of multicast attacks: the fake rendezvous point attack, IGMP flood, and IGMP Leave attacks. The realistic emulation process conducted via GNS3 has provided valuable insights into the intricate mechanisms underlying the execution of these attack.

**PAPER:**

[**https://www.researchgate.net/publication/220955523\_Intrusion\_detection\_with\_OMNeT**](https://www.researchgate.net/publication/220955523_Intrusion_detection_with_OMNeT)

Network simulators serve a variety of purposes. Compared to the cost, time, and effort involved in setting up an entire test bed containing different types of network devices, network simulators are relatively fast and inexpensive. Computer intrusions are occurring almost routinely and have become a major issue in our networked society. Every organization is faced by the big challenge of selecting an intrusion detection system and testing its abilities. Therefore, it is worthwhile to investigate the possibility of implementing and thoroughly testing intrusion detection systems using network simulators. In this paper, we report our experience with implementing and testing intrusion detection systems using OMNeT++ simulator. We highlight how OMNeT++ is harnessed to test and evaluate the intrusion detection system in terms of detection accuracy and performance.

OMNeT++ support for TCP/IP protocols such as Internet Protocol

(IP), Internet Control Message Protocol (ICMP), User Datagram

Protocol (UDP), and Transmission Control Protocol (TCP) started

with the Internet Protocol Suite (IPSuite), and has culminated in

the more recent INET Framework. Both IPSuite and INET

framework have been faithful to the TCP/IP protocol suite with its

layered approach. Several research groups at the University of

Karlsruhe developed MMSim [4] which is a model to simulate

Voice over IP (VoIP) protocols using OMNeT++. The MMSim

model provides support for Session Initiation Protocol (SIP),

Real-time Transmission Protocol (RTP), and Real-Time

Streaming Protocol (RTSP). The modularity that distinguishes

OMNeT++ is reflected on the modeling of networking protocols,

where all components of protocols are divided into a number of

different modules, and each module can have several parameters.

The actual details of each protocol are implemented in C++

programming language, where every major operation of the

protocol is implemented as a member function in the class files

that represent the protocol. All implementations of protocols

follow the specifications detailed in relevant Request for

Comment (RFC) documents.

**References:**

GNS3:

* "GNS3: A Free and Open-Source Network Simulation Software" (2018) - <https://www.researchgate.net/publication/322446788_Using_graphic_network_simulator_3_for_DDoS_attacks_simulation>
* "A Comparative Study of Network Simulation Tools: GNS3, Cisco VIRL, and EVE-NG" (2021) - <https://docplayer.net/51891509-Gns3-network-simulation-guide.html>

Security Onion:

* "Security Onion: A Community-Driven Linux Distribution for Network Security Monitoring" (2014) - <https://blog.securityonion.net/>
* "Evaluating the Effectiveness of Security Onion for Network Intrusion Detection" (2018) - <https://www.researchgate.net/publication/322459826_Semantic_Scholar>

IDS:

* "Intrusion Detection Systems: A Survey and Taxonomy" (2018) - <https://www.researchgate.net/publication/2597023_Intrusion_Detection_Systems_A_Survey_and_Taxonomy>
* "Machine Learning for Intrusion Detection: A Review" (2020) - <https://arxiv.org/abs/2106.09527>

ICMP Flooding Attacks:

* "A Study on Detecting ICMPv6 Flooding Attack based on IDS" (2021) - <https://www.semanticscholar.org/paper/A-Study-on-Detecting-ICMPv6-Flooding-Attack-based-Saad-Ramadass/68b33b4b71dbe9a75f6e4376d7806ee99d6ef751>
* "Detection and Mitigation of ICMP Flooding Attacks in Software-Defined Networks" (2019) - <https://ieeexplore.ieee.org/document/9760911/>

MAC Flooding Attack:

* "MAC Address Flooding Attack Detection and Mitigation Techniques: A Survey" (2020) - <https://ieeexplore.ieee.org/document/10142764/>
* "A Novel Approach for Detecting and Mitigating MAC Flooding Attacks in Wireless Networks" (2021) - <https://orbilu.uni.lu/handle/10993/53373>

TCP SYN DoS Attack:

* "Defense against SYN Flood Attacks: A Survey" (2017) - <https://arxiv.org/abs/2211.15404>
* "Mitigating SYN Flood Attacks with Enhanced Queue Management Techniques" (2019) - <https://arxiv.org/abs/2312.02102>

UDP Flooding Attack:

* "UDP Flood Attack Detection and Mitigation Techniques: A Review" (2021) - <https://arxiv.org/abs/2004.04676>
* "A Collaborative Approach for Detecting and Mitigating UDP Flooding Attacks in Cloud Environments" (2020) - <https://arxiv.org/abs/1908.00090>

**Inference:**

Implementing an Intrusion Detection System in GNS3 with Security Onion and Monitoring with Wireshark

In this project, we successfully implemented an Intrusion Detection System (IDS) within GNS3 utilizing Security Onion and monitored its effectiveness with Wireshark. The achieved results demonstrate the feasibility and effectiveness of this approach for detecting and mitigating network security threats.

**Key Findings:**

Security Onion, coupled with GNS3 and Wireshark, offers a powerful and user-friendly environment for deploying and monitoring IDS solutions.

The implemented IDS effectively detected various simulated cyberattacks, including network scans, port scans, and denial-of-service (DoS) attacks.

Wireshark provided valuable insights into network traffic, facilitating the identification of suspicious activity and confirming IDS alerts.

The combined use of these open-source tools allows for cost-effective and flexible IDS implementation, making it accessible to individual researchers, small businesses, and educational institutions.

**Conclusion:**

Implementing an IDS using Security Onion and GNS3, and monitoring it with Wireshark, proved to be a successful approach for enhancing network security. This setup provides a valuable tool for detecting and mitigating various cyberattacks, offering a cost-effective and customizable solution for security professionals. The acquired knowledge and experience gained through this project can be applied to real-world network security scenarios, further strengthening cybersecurity measures and protecting critical infrastructure.

**Future Work:**

Several potential avenues exist for further exploration and improvement. One key area is expanding the scope of simulated cyberattacks to include more complex and advanced scenarios. Additionally, integrating Security Onion with other security tools could enhance its overall detection and response capabilities. Finally, conducting further research on IDS optimization techniques could yield improvements in performance and resource utilization.

By continuing research and development in this area, we can ensure that IDS solutions remain effective in the face of evolving cyber threats. Together, we can create a safer and more secure digital world for all.

**References :**

**GNS3:**

* **Official Website:**[**https://www.gns3.com/software**](https://www.gns3.com/software)
* **Documentation:**[**https://docs.gns3.com/**](https://docs.gns3.com/)
* **Download:**[**https://www.gns3.com/software**](https://www.gns3.com/software)
* **Community:**[**http://forum.gns3.net/**](http://forum.gns3.net/)

**Security Onion:**

* **Official Website:**[**https://blog.securityonion.net/**](https://blog.securityonion.net/)
* **Documentation:**[**https://docs.securityonion.net/**](https://docs.securityonion.net/)
* **Downloads:**[**https://securityonionsolutions.com/software/**](https://securityonionsolutions.com/software/)
* **Community:**[**https://blog.securityonion.net/**](https://blog.securityonion.net/)

**IDS:**

* **Wikipedia:**[**https://en.wikipedia.org/wiki/Intrusion\_detection\_system**](https://en.wikipedia.org/wiki/Intrusion_detection_system)
* **SANS Institute:**[**https://www.sans.org/white-papers/337/**](https://www.sans.org/white-papers/337/)
* **Cisco:**[**https://www.cisco.com/c/en/us/products/security/ngips/index.html**](https://www.cisco.com/c/en/us/products/security/ngips/index.html)
* **Fortinet:**[**https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system**](https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system)

**ICMP Flooding Attacks:**

* **Wikipedia:**[**https://en.wikipedia.org/wiki/Ping\_of\_death**](https://en.wikipedia.org/wiki/Ping_of_death)
* **Imperva:**[**https://www.imperva.com/blog/the-3-biggest-ddos-attacks-imperva-has-mitigated/**](https://www.imperva.com/blog/the-3-biggest-ddos-attacks-imperva-has-mitigated/)
* **Palo Alto Networks:**[**https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMRqCAO&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail**](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMRqCAO&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail)

**MAC Flooding Attack:**

* **Wikipedia:**[**https://en.wikipedia.org/wiki/MAC\_flooding**](https://en.wikipedia.org/wiki/MAC_flooding)
* **CyberArk:**[**https://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php**](https://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php)
* **Fortinet:**[**https://docs.fortinet.com/document/fortigate/6.2.15/cookbook/771644/dos-protection**](https://docs.fortinet.com/document/fortigate/6.2.15/cookbook/771644/dos-protection)

**TCP SYN DoS Attack:**

* **Wikipedia:**[**https://en.wikipedia.org/wiki/SYN\_flood**](https://en.wikipedia.org/wiki/SYN_flood)
* **Cloudflare:**[**https://community.cloudflare.com/t/direct-syn-flood-attack-mitigation-with-cloudflare/271636**](https://community.cloudflare.com/t/direct-syn-flood-attack-mitigation-with-cloudflare/271636)
* **Imperva:**[**https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/**](https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/)

**UDP Flooding Attack:**

* **Wikipedia:**[**https://en.wikipedia.org/wiki/UDP\_flood\_attack**](https://en.wikipedia.org/wiki/UDP_flood_attack)
* **A10 Networks:**[**https://www.a10networks.com/blog/understanding-ddos-attacks/**](https://www.a10networks.com/blog/understanding-ddos-attacks/)
* **Imperva:**[**https://www.imperva.com/blog/ceoblog/**](https://www.imperva.com/blog/ceoblog/)