Enterprise Security Threat Detection & Prevention System

Submit by

KASHYAP V.P

Objective

To develop a cybersecurity framework that focuses on network security, web security, cloud security, and compliance monitoring, using modern tool Wazuh

Approach

- Set up a virtual cyber security lab.
- Research common enterprise threats and frameworks.
- Deploy SIEM and security solutions.
- Simulate attacks and observe detection capabilities.

Tools

- Virtual Machines: Kali Linux, Ubuntu
- Security Tools: Wazuh, Splunk, ELK Stack, Sysmon, Snort, Suricata
- Others: Sigma, YARA, Windows Defender Firewall, iptables

Weekly Logs

Week 1: Introduction to Enterprise Security Threats

Activities Performed

Researched common threats

Malware

Malware (short for "malicious software") refers to any software intentionally designed to cause damage to a computer, server, client, or computer network. There are several types of malware:

- **Viruses**: Programs that replicate themselves and spread to other files
- **Trojans**: Software that pretends to be legitimate but has malicious intent.
- **Worms**: Similar to viruses, but they can spread independently across networks.
- **Spyware**: Software that collects information about a user without their knowledge.
- **Adware**: Software that automatically displays or downloads unwanted ads.

Phishing

Phishing is a type of cyberattack that uses fake emails, websites, or messages to deceive users into revealing sensitive information, such as usernames, passwords, or credit card numbers. Phishing can come in several forms:

- **Spear phishing**: A targeted attack, often aimed at individuals or companies.
- **Whaling**: A form of phishing targeting high-profile individuals like executives or leaders.
- **Vishing**: Voice phishing, typically done over the phone.

Ransomware

Ransomware is a type of malware that locks or encrypts a user's data, and the attacker demands payment (usually in cryptocurrency) in exchange for restoring access. Common examples include **WannaCry** and **Petya**

DDoS (Distributed Denial of Service)

DDoS attacks involve overwhelming a server, service, or network with a flood of internet traffic to render the target unusable. These attacks are carried out using a network of infected devices, called a botnet, which causes a massive surge in traffic

Insider Threats

Insider threats occur when individuals within an organization (employees, contractors, etc.) intentionally or unintentionally cause harm to the organization. This harm could be through data theft, sabotage, or accidental leaks

Basic Security Frameworks

NIST (National Institute of Standards and Technology)

NIST also provides several guidelines, including those on risk management (NIST SP 800-53) and secure software development. NIST provides a comprehensive framework for improving cybersecurity across critical infrastructure. Its **Cybersecurity Framework (CSF)** helps organizations identify, assess, and manage cybersecurity risks. The CSF is made up of five core functions:

- **Identify**: Develop an understanding of the organization's assets, risks, and resources.
- **Protect**: Implement safeguards to prevent cyber threats.
- **Detect**: Identify cybersecurity events in real-time.
- **Respond**: Develop strategies to mitigate and respond to incidents.
- **Recover**: Plan for recovery and restoration of any lost or damaged assets.

ISO 27001

ISO 27001 is an international standard for managing information security. The focus of the ISO 27001 standard is on establishing, implementing, operating, monitoring, reviewing, and maintaining an Information Security Management System (ISMS). Key components include:

- **Information Security Policy**: A strategic document to set the direction for security within an organization.
- **Risk Assessment and Treatment**: Identifying risks to information security and implementing measures to mitigate them.

Control Objectives: Specific security measures and practices that need to be in place, such as access controls and physical security

CIS Controls

The **Center for Internet Security (CIS)** provides a set of **CIS Controls** that organizations can implement to protect against the most common and damaging cybersecurity threats. These controls are divided into three categories:

1. **Basic Controls**: Such as inventory and control of hardware/software, continuous vulnerability management, and controlled use of administrative privileges.
2. **Foundational Controls**: These include email and web browser protections, malware defenses, and data recovery capabilities.
3. **Organizational Controls**: These focus on incident response and security awareness training.

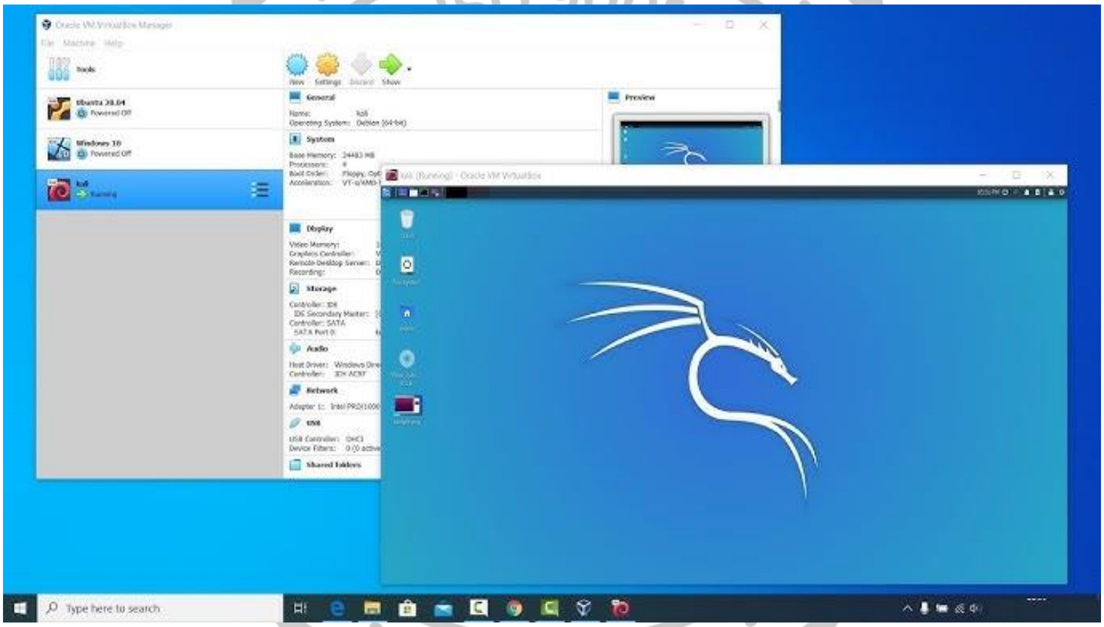
These frameworks and controls serve as foundational tools in designing and implementing an effective cybersecurity strategy

Set up Virtual Lab Environment Set up Virtual Lab Environment

-
    - Installed **Kali Linux**, **Ubuntu** on VirtualBox.

Challenges Faced

Ubuntu download delays (resolved with a faster mirror).



General
Name: kali
Operating System: Debian (64-bit)

System
Base Memory: 24483 MB
Processors: 4
Boot Order: Floppy, Opt
Acceleration: VT-x/AMD-

Display
Video Memory:
Graphics Controller:
Remote Desktop Server:
Recording:

Storage
Controller: IDE
IDE Secondary Master:
Controller: SATA
SATA Port 0:

Audio
Host Driver: Windows Dire
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000

USB
USB Controller: OHCI
Device Filters: 0 (0 active

Shared Folders

Week 2: Logging & Monitoring

Activities Performed

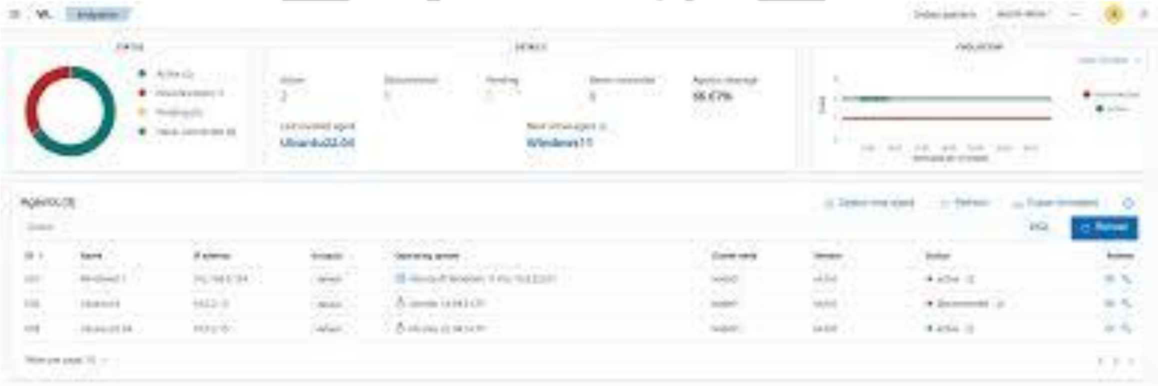
Installed **Wazuh** and Wazuh agent on Ubuntu

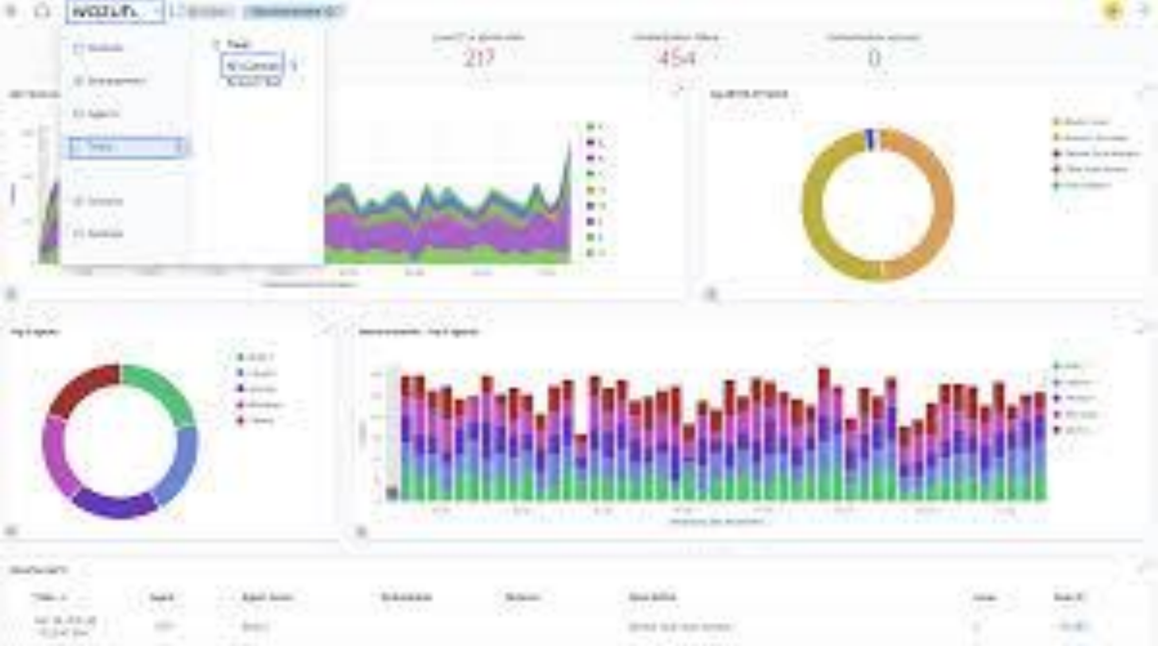
Collected and analyzed sample system logs:

- Detected login events, privilege escalation attempts.

Challenges Faced

Initial Wazuh installation failed due to missing dependencies (fixed by installing required packages manually).





Week 3: Firewall & Endpoint Security

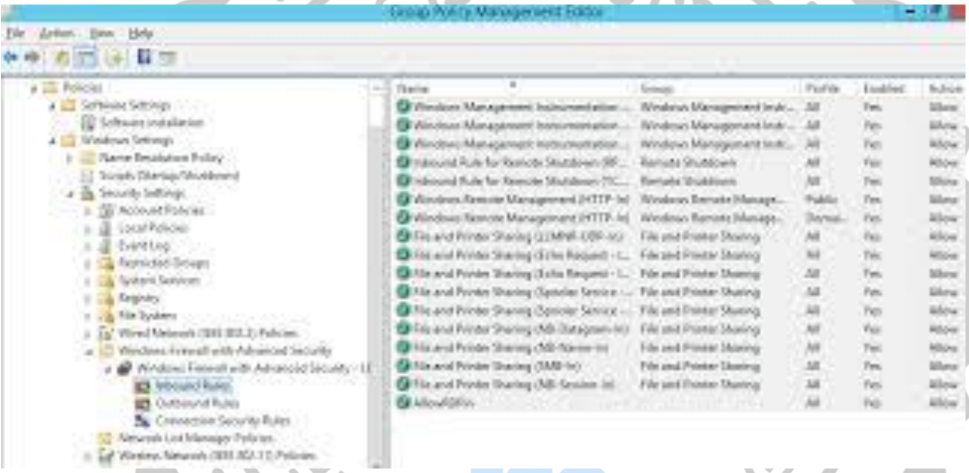
Activities Performed

- Configured **Windows Defender Firewall** to block all inbound connections except RDP.

- Set up **iptables** rules on Ubuntu to allow only SSH.

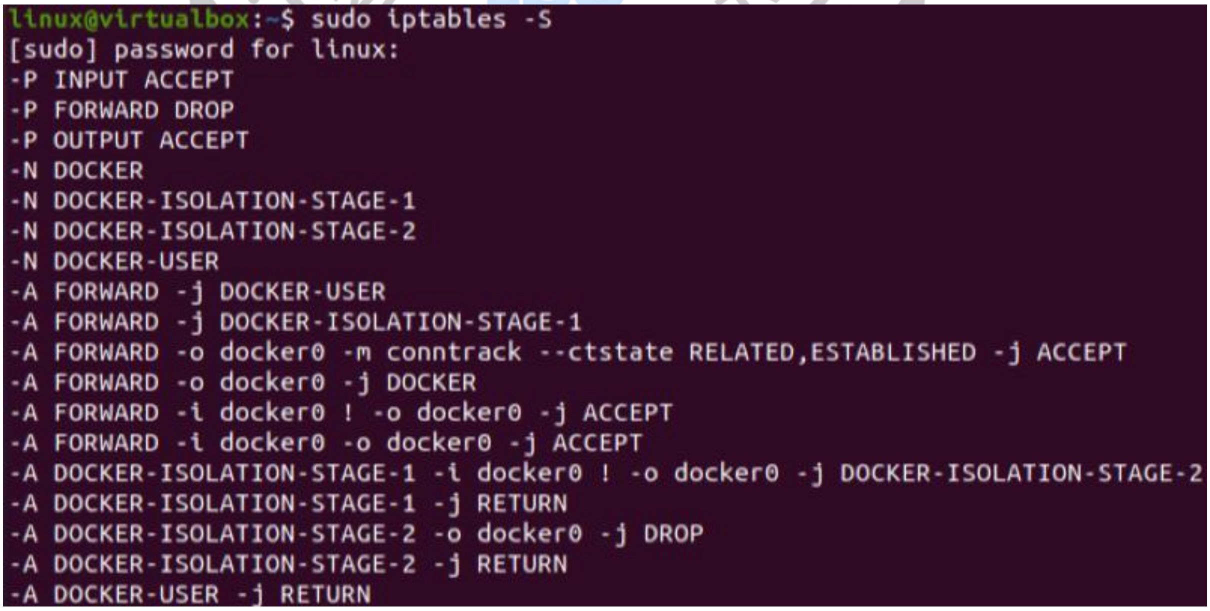
Challenges Faced

- iptables rules misconfiguration blocked SSH (resolved by allowing SSH before applying other rules).


Group Policy Management Editor
File
Action
View
Help
Policies
Software Settings
Software installation
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security - L
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies

Name	Group	Profile	Enabled	Action
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Allow
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Allow
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Allow
Inbound Rule for Remote Shutdown (RP...	Remote Shutdown	All	Yes	Allow
Inbound Rule for Remote Shutdown (TC...	Remote Shutdown	All	Yes	Allow
Windows Remote Management (HTTP-In)	Windows Remote Manage...	Public	Yes	Allow
Windows Remote Management (HTTP-In)	Windows Remote Manage...	Domai...	Yes	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Spooler Service - ...	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Spooler Service - ...	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Allow
AllowRDPin		All	Yes	Allow

-



```
linux@virtualbox:~$ sudo iptables -S
[sudo] password for linux:
-P INPUT ACCEPT
-P FORWARD DROP
-P OUTPUT ACCEPT
-N DOCKER
-N DOCKER-ISOLATION-STAGE-1
-N DOCKER-ISOLATION-STAGE-2
-N DOCKER-USER
-A FORWARD -j DOCKER-USER
-A FORWARD -j DOCKER-ISOLATION-STAGE-1
-A FORWARD -o docker0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -o docker0 -j DOCKER
-A FORWARD -i docker0 ! -o docker0 -j ACCEPT
-A FORWARD -i docker0 -o docker0 -j ACCEPT
-A DOCKER-ISOLATION-STAGE-1 -i docker0 ! -o docker0 -j DOCKER-ISOLATION-STAGE-2
-A DOCKER-ISOLATION-STAGE-1 -j RETURN
-A DOCKER-ISOLATION-STAGE-2 -o docker0 -j DROP
-A DOCKER-ISOLATION-STAGE-2 -j RETURN
-A DOCKER-USER -j RETURN
```

Final Security Report

Threat Landscape Analysis

Modern enterprise environments face multiple threats such as malware, phishing, ransomware, DDoS attacks, and insider threats. These threats exploit vulnerabilities in system configurations, network defenses, and user awareness.

Implementation Details

- Virtual Lab established with Kali, Ubuntu, and Wazuh
- Wazuh and Splunk configured as SIEM solutions.
- Firewalls and IDS/IPS configured to block unauthorized access and detect intrusions.

Test Results & Attack Simulations

- **Brute Force Attack** detected successfully by Wazuh.
- **Malware Execution (EICAR)** triggered Wazuh alarm.
- **Firewall rules** effectively blocked unauthorized connection attempts.