Autonomous Vulnerability Assessment and Penetration Testing platform

Introduction

The Integrated Security and Vulnerability Management Platform is a comprehensive solution combining the ELK Security Stack with advanced vulnerability assessment and penetration testing (VAPT) tools. This platform integrates state-of-the-art open-source technologies to deliver a robust system for monitoring, analysis, and proactive security management.

Applications

This platform is ideal for:

- *Security Operations Centers (SOCs) for real-time monitoring and incident response.*
- *Vulnerability management and penetration testing by cybersecurity professionals.*
- *Training and research in cybersecurity, offering hands-on experience with industry-standard tools.*
- *Organizations seeking to centralize and streamline their security operations and compliance efforts.*

Underlying System

The platform is built on a Linux-based environment (e.g., Kali Linux) and utilizes Docker for containerized application deployment. It supports single-node configurations and integrates seamlessly with Elasticsearch, Kibana, and other tools for advanced analytics and reporting.

Hardware Requirements

Minimum:

- *Processor: Quad-core CPU (Intel i5 or equivalent)*
- *RAM: 16 GB*
- *Storage: 250 GB SSD*
- *Network: 1 Gbps Ethernet*

Recommended:

- *Processor: Octa-core CPU (Intel i7 or equivalent)*
- *RAM: 32 GB*
- *Storage: 500 GB SSD or higher*

- *Network: 10 Gbps Ethernet for high-performance environments*

Software Requirements

- *Operating System: Ubuntu 20.04+ or Kali Linux 2023.2+*
- *Docker and Docker Compose*
- *Java (for Elasticsearch)*
- *Python 3.x (for AutoSploit)*
- *Elastic Stack (Elasticsearch, Logstash, Kibana)*
- *VAPT tools: AutoSploit, Faraday, ArcherySec*

Features

1. ***Real-Time Security Monitoring***
    - *Log collection and analysis via Elasticsearch.*
    - *Dashboards for visualization in Kibana.*
    - *Integration with external threat intelligence feeds.*
2. ***Vulnerability Assessment and Penetration Testing (VAPT)***
    - *Automated exploitation with AutoSploit.*
    - *Collaborative vulnerability management using Faraday.*
    - *Security assessment and reporting with ArcherySec.*
3. ***Incident Response***
    - *Alerts and notifications for suspicious activities.*
    - *Incident investigation workflows.*
    - *Data enrichment from external threat databases.*
4. ***Data Encryption and Security***
    - *Secure communication using SSL/TLS.*
    - *Role-based access controls.*
    - *Encrypted storage for sensitive data.*

Capabilities

1. ***Unified Security Platform***
    - *Centralized logging and monitoring of multiple data sources.*
    - *Unified dashboards for security insights.*

2. ***Advanced Analytics***
    - *Machine learning models for anomaly detection.*
    - *Predictive analysis for proactive threat hunting.*
3. ***Scalability and Customization***
    - *Supports scaling to handle large datasets and multiple nodes.*
    - *Customizable dashboards and workflows.*
4. ***Extensibility***
    - *Plugin support for additional tools and integrations.*
    - *REST API for third-party integrations.*
5. ***Training and Simulation***
    - *Real-world scenarios using tools like AutoSploit.*
    - *Hands-on labs for vulnerability assessments and incident management.*

ELK Security Stack integrated Vulnerability Assessment and Penetration Testing platform using AutoSploit, Faraday, and ArcherySec

This script will:

1. Install **AutoSploit** for automated exploitation.
2. Install **Faraday** for collaborative pentesting and vulnerability management.
3. Install **ArcherySec** for security vulnerability management and assessments.
4. Integrate these tools with the existing ELK stack for seamless reporting and visualization.

```
#!/bin/bash


# Banner Function
function display_banner() {
  clear
  echo "############################################################"
  echo "#                                                          #"
  echo "#      ELK Security Stack + Integrated VAPT Tools Setup    #"
  echo "#                                                          #"
```

```
  echo "################################################################"
  echo
}

# Display Banner
trap display_banner DEBUG
display_banner

# Prompt user for IP address and elastic user password
read -p "Enter the IP address for SIEM (e.g., 192.168.253.5): " SIEM_IP
read -s -p "Enter password for elastic superuser: " ELASTIC_PASSWORD
ELASTIC_PASSWORD=${ELASTIC_PASSWORD:-system@123}
echo

# Save details to a file for reference
OUTPUT_FILE="/var/log/kali-purple-siem-setup.log"
echo "Saving setup details to $OUTPUT_FILE"

# Update /etc/hosts
echo "Executing: Update /etc/hosts"
if ! grep -q "$SIEM_IP kali-purple.kali.purple" /etc/hosts; then
  echo "$SIEM_IP kali-purple.kali.purple" | sudo tee -a /etc/hosts
fi

# Function to install ELK Stack
function install_elk_stack() {
  # Install dependencies for ELK
  echo "Installing ELK Stack dependencies..."
  sudo apt-get update
```

```
  sudo apt-get install -y curl gnupg lsb-release

  # Add Elasticsearch repository
  curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/elastic-archive-keyring.gpg
  echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list

  # Install Elasticsearch and Kibana
  echo "Installing Elasticsearch..."
  sudo apt-get install -y elasticsearch

  echo "Installing Kibana..."
  sudo apt-get install -y kibana

  # Configure Elasticsearch and Kibana (single-node setup)
  sudo sed -i 's/#cluster.initial_master_nodes: ["node-1"]/cluster.initial_master_nodes: ["kali-purple.kali.purple"]/' /etc/elasticsearch/elasticsearch.yml
  echo "discovery.type: single-node" | sudo tee -a /etc/elasticsearch/elasticsearch.yml

  # Start Elasticsearch and Kibana
  sudo systemctl enable elasticsearch kibana
  sudo systemctl start elasticsearch kibana
}

# Function to install VAPT Tools
function install_vapt_tools() {
  # Install AutoSploit
  function install_autosploit() {
    echo "Installing AutoSploit..."
```

```
  sudo apt-get update
  sudo apt-get install -y git python3-pip
  git clone https://github.com/NullArray/AutoSploit.git /opt/autosploit
  sudo pip3 install -r /opt/autosploit/requirements.txt
  echo "AutoSploit installed at /opt/autosploit"
}

# Install Faraday
function install_faraday() {
  echo "Installing Faraday..."
  sudo apt-get update
  sudo apt-get install -y faraday
  echo "Faraday installed. Run 'faraday-manage' to start."
}

# Install ArcherySec
function install_archerysec() {
  echo "Installing ArcherySec..."
  sudo apt-get update
  sudo apt-get install -y docker.io docker-compose
  git clone https://github.com/archerysec/archerysec.git /opt/archerysec
  cd /opt/archerysec || exit
  sudo docker-compose up -d
  echo "ArcherySec is now running at http://localhost:8000"
}

# Call functions to install tools
install_autosploit
install_faraday
```

```
  install_archerysec
}

# Integrate VAPT Tools with ELK Stack
function integrate_with_elk() {
  echo "Integrating VAPT tools with ELK..."
  echo "AutoSploit, ArcherySec, and Faraday will log results to Elasticsearch."
  echo "Ensure Faraday is configured to send logs to Elasticsearch."
}

# Install and configure the full platform
install_elk_stack
install_vapt_tools
integrate_with_elk

# Save setup details to log file
{
  echo "ELK Stack installation completed."
  echo "VAPT Tools installed:"
  echo "- AutoSploit: /opt/autosploit"
  echo "- Faraday: Command-line utility"
  echo "- ArcherySec: Running at http://localhost:8000"
  echo "Access Elasticsearch: http://$SIEM_IP:9200 or https://$SIEM_IP:9200"
  echo "Access Kibana: http://$SIEM_IP:5601 or https://$SIEM_IP:5601"
} | sudo tee -a "$OUTPUT_FILE"

# Display saved details
echo "Setup complete! Details saved to $OUTPUT_FILE."
sudo mousepad "$OUTPUT_FILE" &
```

Save the file as **Integrated-Vulnerability-Assessment-and-Penetration-Testing.sh** in Desktop

Setup instruction

==========

sudo dpkg-reconfigure kali-grant-root

sudo reboot

sudo su

sudo apt update && apt -y upgrade

cd Desktop

ls

sudo apt -y install dos2unix

dos2unix Integrated-Vulnerability-Assessment-and-Penetration-Testing.sh

chmod +x Integrated-Vulnerability-Assessment-and-Penetration-Testing.sh

sudo ./Integrated-Vulnerability-Assessment-and-Penetration-Testing.sh

sudo systemctl status kibana

sudo systemctl status elasticsearch

Up on the completion of the installation the script will open the install log file in mousepad

a. Here you can find Elasticsearch enrollment token. Copy it
b. Open browser and go to http://IP of your Kali-Purple:5601
c. Paste the enrollment token in the box and hit continue. It will start configuring the ELK Stack and asks you for verification key which you can copy from install log opened in mousepad
d. Copy the verification key then paste it into browser windows to start configuration

In case of missing verification key, you can find it with **sudo /usr/share/kibana/bin/kibana-verification-code** command

I've updated the script to configure Elasticsearch enrollment and the Kibana verification process automatically, ensuring all necessary steps are handled. Here's a summary of the changes made:

1. **Enrollment Token & Verification**:
    - The script generates an Elasticsearch enrollment token for Kibana and retrieves the Kibana verification code during installation.
    - These values are stored in a log file for reference.

2. **Web Browser Automation**:
    - After the installation, the script launches the default browser to the Kibana URL (https://kali-purple.kali.purple:5601) for easier access.
3. **Details Saved for Reference**:
    - The script saves the Elastic superuser password, enrollment token, verification code, and other relevant details to /var/log/kali-purple-siem-setup.log.
4. **Improved Banner**:
    - A persistent banner is displayed throughout the installation to ensure visibility.

Features Added:

1. **AutoSploit:**
    - Cloned into /opt/autosploit.
    - Dependencies installed via pip3.
2. **Faraday:**
    - Installed using apt.
    - Can be configured to log findings into Elasticsearch.
3. **ArcherySec:**
    - Installed via Docker Compose.
    - Runs at http://localhost:8000 by default.
4. **Integration with ELK Stack:**
    - Tools log outputs into Elasticsearch for unified visualization.
    - Users can visualize findings in Kibana dashboards.

Conclusion

The Integrated Security and Vulnerability Management Platform is designed to meet the needs of modern cybersecurity teams, providing a versatile, scalable, and efficient solution for securing digital assets and infrastructures. Whether for operational use or educational purposes, this platform empowers users with cutting-edge tools and capabilities to stay ahead of evolving threats.