Cyber Security Assignment-8 Questions

P LOHENDRA

2406CYS124

Question – 1

1.Imagine you are a cybersecurity analyst working for a large multinational corporation. One morning, your team receives an urgent report about a potential security breach in the company's network. The IT department has noticed unusual network activity originating from a particular IP address. Your team has been tasked with investigating this incident to determine if it poses a threat to the organization's network security.

Assignment Question:

I. Using the Python library Scapy, analyze the network packets associated with the suspicious IP address provided.

Expected Procedure:

1. A detailed explanation of how Scapy can be utilized to capture and dissect network packets.
2. A step-by-step breakdown of the process you followed to capture and analyze the network traffic.
3. Identification and interpretation of any suspicious or anomalous network behavior observed in the captured packets.
4. Recommendations for mitigating the identified security risks and securing the network against similar threats in the future.

Expected Code:

1. Write a python code to Network Packet Analysis with Scapy

Question – 2

2.Imagine you are working as a cybersecurity analyst at a prestigious firm. Recently, your company has been experiencing a surge in cyber attacks, particularly through phishing emails and websites. These attacks have not only compromised sensitive information but also tarnished the reputation of the company.

In light of these events, your team has been tasked with developing a robust solution to detect and mitigate phishing websites effectively. Leveraging your expertise in Python programming and cybersecurity, your goal is to create a program that can accurately identify phishing websites based on various features and indicators.

Assignment Task:

Using the Python programming language, develop a phishing website detection system that analyzes website characteristics and determines the likelihood of it being a phishing site.

Expected Procedure:

1. Accept 2 web URL One real and another one phishing.
2. Analyze the data from both the websites.
3. Identify the phishing site.

Expected Code:

1.Phishing Website Detection with Python

Answers:

Answer for first question:-

Cybersecurity Breach Response Protocol

I. Report Verification

Upon receiving a report of unusual network activity, I initiate a thorough verification process. This entails scrutinizing network logs, traffic data, and other pertinent records to ascertain the authenticity of the alert.

II. Information Collection

I proceed to amass comprehensive details about the flagged IP address. This includes pinpointing its geographical origin, ownership, any ties to known cyber threats, and a history of related security incidents.

III. Network Traffic Analysis

Employing network surveillance and intrusion detection tools, I dissect the data flow from the questionable IP. I look for traffic types, utilized ports, communication trends, and irregularities that suggest nefarious activities like port scans, data theft, or intrusion attempts.

IV. Endpoint Inspection

A meticulous examination of network endpoints is conducted to uncover any traces of compromise or infection. This covers an audit of abnormal processes, file changes, unauthorized entries, and other signs of security breaches.

V. Threat Intelligence Utilization

I harness intelligence from various feeds and databases to learn about prevalent dangers linked to the suspicious IP, such as malware footprints, control servers, and other red flags.

VI. Threat Containment & Mitigation

Should the inquiry validate a cyber threat, I collaborate with IT to neutralize the risk. This involves severing connections with the harmful IP, deactivating affected accounts or systems, and fortifying security measures to block further infiltrations or data leaks.

VII. Forensic Investigation

Simultaneously, I engage in forensic scrutiny to collect evidence and gauge the breach's scope. This includes preserving and studying logs, system snapshots, memory captures, and additional data to pinpoint the incursion's source and its repercussions on network integrity.

VIII. Incident Response Execution

Throughout the probe, I adhere to the predefined incident response strategy, liaising with departments like IT, legal, and executive management to guarantee a unified and efficacious resolution to the security incident.

IX. Documentation & Communication

In conclusion, I compile a detailed account of the findings, measures implemented, and suggestions for bolstering security. This report is disseminated among principal parties to refine the organization's defensive stance and response readiness for future incidents.

Python

```python
from scapy.all import *

# Define the IP address to monitor
suspicious_ip = '192.168.1.100'

# Capture packets
packets = sniff(filter=f'ip src {suspicious_ip}', count=10)

# Analyze packets
for packet in packets:
    # Print packet summary
    print(packet.summary())
    # More detailed analysis can be done here, such as:
    # - Checking for unusual protocols
    # - Inspecting payload data
    # - Identifying patterns indicative of malicious activity

# Recommendations:
# - Ensure all systems are updated with the latest security patches.
# - Implement network segmentation to limit the spread of potential breaches.
# - Use intrusion detection systems (IDS) to monitor network traffic.
```

Answer for Question 2)

Web Scraping and Analysis:

1. **Import Libraries:** Use requests and beautifulsoup4 for web scraping.
2. **Input URLs:** Prompt for two URLs - one legitimate, one potentially phishing.

Data Fetching and Analysis: 3. **Fetch HTML:** Retrieve website content using requests. 4. **Parse HTML:** Analyze content with beautifulsoup4, checking for suspicious elements and SSL/TLS certificates.

Heuristics and Feature Comparison: 5. **Apply Heuristics:** Identify phishing indicators, such as URL anomalies. 6. **Examine Features:** Assess domain registration length, SSL validity, specific HTML elements, external links, and email addresses.

Phishing Score Calculation: 7. **Assign Weights:** Prioritize features by importance. 8. **Calculate Scores:** Sum weighted features for each URL.

Model Building and Evaluation: 9. **Build Model:** Train a classification model with algorithms like logistic regression. 10. **Feature Engineering:** Prepare website characteristics for the model. 11. **Train and Evaluate:** Split data, train the model, and assess performance.

Prediction and Display: 12. **Predict Phishing:** Use the model to evaluate new URLs. 13. **Display Results:** Show predictions and supporting evidence.

This streamlined process outlines the steps for detecting phishing websites using web scraping, data analysis, and machine learning.

Python

```python
import requests
from bs4 import BeautifulSoup

# URLs to analyze
real_url = 'https://www.example.com'
phishing_url = 'https://www.phishingexample.com'

# Function to analyze website content
def analyze_website(url):
    try:
        response = requests.get(url)
        soup = BeautifulSoup(response.text, 'html.parser')
        # Analyze website features such as URL structure, SSL certificate, content, etc.
        # This is a simplified example
        if 'login' in soup.text.lower():
            print(f'{url} might be a phishing site.')
        else:
            print(f'{url} seems legitimate.')
    except requests.exceptions.RequestException as e:
        print(f'Error analyzing {url}: {e}')

# Analyze both websites
analyze_website(real_url)
analyze_website(phishing_url)

# Recommendations:
# - Educate employees about phishing and how to recognize suspicious websites.
# - Implement anti-phishing tools and browser extensions.
# - Regularly update blacklists of known phishing sites.
```