SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit II- E-MAIL SECURITY & FIREWALLS

Topic : The Role of Firewalls in Cyber Forensics

INTRODUCTION

Firewalls, as a critical line of defense, play a multifaceted role in cyber defense & forensics , both in preventing attacks and providing valuable forensic data. This presentation will explore how firewalls contribute to cyber forensics, from their preventative capabilities to the crucial information they log and retain.

Firewalls as Digital Evidence

Network Activity

Firewalls monitor and record all network traffic. This activity creates a detailed log of connections and data flow.

Access Attempts

Logs capture successful and failed access attempts. This can identify unauthorized access and potential breaches.

Data Transfer

Firewalls track data entering and leaving the network. This information reveals potential data exfiltration.

Leveraging Firewall Logs for Incident Response

1 Identify the Source

Firewall logs pinpoint the origin of an attack. This helps in tracing malicious activities.

2 Contain the Damage

Quickly block malicious traffic. Limiting the spread of the incident across the network.

3 Analyze the Impact

Review logs to understand what systems were affected. Determine the extent of the data breach.

Preventing Cybercrimes with Firewalls

Traffic Filtering

Firewalls filter network traffic based on rules. Blocking known malicious IP addresses and ports.

Access Control

Limiting network access to authorized users. Preventing unauthorized access to sensitive data.

Content Inspection

Examining the content of network traffic. Detecting and blocking malicious code or data.

Intrusion Detection & Prevention

1

Signature-Based

Detecting known attack patterns. Matching traffic against a database of signatures.

2

Anomaly-Based

Identifying unusual network behavior. Flagging deviations from normal traffic patterns.

3

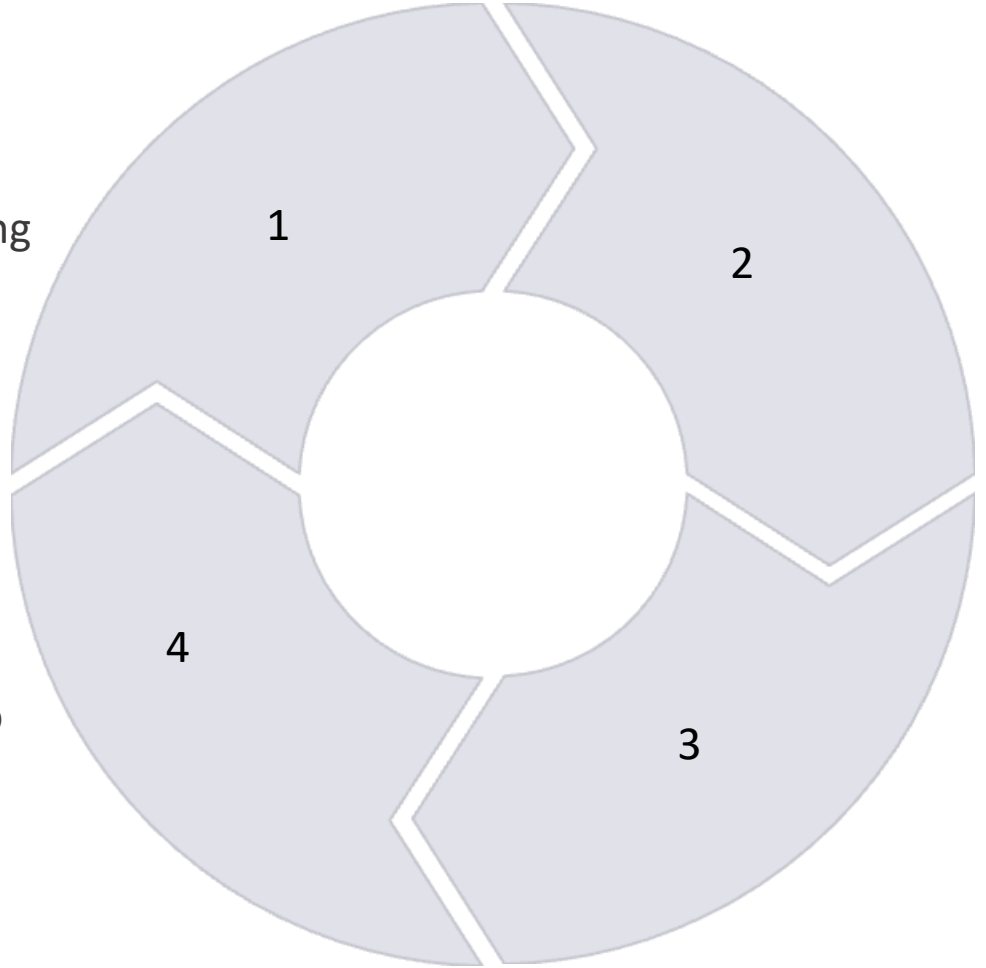
Heuristic-Based

Analyzing traffic for suspicious characteristics. Using rules and algorithms to detect attacks.

Firewall Forensic Investigation Techniques

Log Analysis

Reviewing firewall logs. Identifying suspicious activity.



Configuration Review

Examining firewall settings. Identifying vulnerabilities.

Correlation

Correlating firewall data. Linking to other events.

Traffic Analysis

Analyzing network traffic. Detecting malicious patterns.

Challenges in Firewall Forensics

Log Volume

Massive log files. Difficult to sift through for relevant data.

Log Rotation

Logs are overwritten. Losing crucial historical information.

Tampering

Logs can be altered. Making evidence unreliable.

Legal and Compliance Considerations

1

Data Privacy

Protecting personal information. Adhering to privacy regulations.

2

Evidence Admissibility

Ensuring data integrity. Following chain of custody procedures.

3

Regulatory Compliance

Meeting industry standards. Complying with legal requirements.

Any Query????

Thank you……